

Relatie tussen factoren van trustworthiness en IT-outsourcing risico's: Wat is de invloed van deze relaties op vertrouwen?

Relatie tussen factoren van trustworthiness en IT-outsourcing risico's

Wat is de invloed van deze relaties op vertrouwen?

Student: Leonie Hendriks

Identiteitsnummer: 851199058

Datum rapport: 25 mei 2017

Datum presentatie: 27 juni 2017

Relation between factors of trustworthiness and IT-outsourcing risks: What is the influence of these relations on trust?

Relation between factors of trustworthiness and IT-outsourcing risks

What is the influence of these relations on trust?

Opleiding: Open Universiteit, faculteit Management, Science & Technology
Masteropleiding Business Process Management & IT

Programme: Open University of the Netherlands, faculty of Management, Science & Technology
Master Business Process Management & IT

Cursus: IM9806 Afstudeertraject Business Process Management and IT

Student: Leonie Hendriks

Identiteitsnummer: 851199058

Datum: 25 mei 2017

Afstudeerbegeleider: dr. ir. Werner (W.G.M.M.) Rutten / prof. dr. Rob (R.J.) Kusters

Meelezer: dr.ir. Harry (H.) Martin

Derde beoordelaar: n.v.t.

Versienummer: 1.0

Status: Definitief

Abstract

Vertrouwen is een veel onderzocht onderwerp binnen de sociale- en psychologische wetenschap. Ook zakelijk gedrag wordt steeds meer getracht te verklaren door middel van vertrouwen. In dit onderzoek wordt getracht een antwoord te geven op de vraag of factoren van trustworthiness invloed hebben op IT-outsourcing risico's (ITO-risico's). Deze vraag is relevant omdat middels beïnvloeding van de factoren van trustworthiness er gestuurd zou kunnen worden op de ITO-risico's om de perceptie van deze risico's te reduceren.

Middels interviews met drie respondenten is de relatie, mate van invloed en sterkte van deze invloed, tussen de factoren van trustworthiness en ITO-risico's bevraagd. De twee belangrijkste conclusies zijn dat de factoren van trustworthiness van Mayer (1995) daadwerkelijk van invloed zijn op de ITO-risico's en dat de sterkte van deze invloed correleert met de mate van invloed van deze factoren op het risico.

Sleutelbegrippen

Vertrouwen, Trust, IT-outsourcing, factoren van trustworthiness, relatie, invloed

Samenvatting

“The best way to find out if you can trust somebody is to trust them.”

- Ernest Hemingway

Vertrouwen is een veel onderzocht onderwerp binnen de sociale- en psychologische wetenschap. Ook zakelijk gedrag wordt steeds meer getracht te verklaren door middel van vertrouwen (Earle, 2010). Maar wat is vertrouwen en hoe wordt dit gemeten? Kan er bewust gestuurd worden op factoren van trustworthiness en kan hierdoor de perceptie van gedefinieerde risico's binnen IT-outsourcing trajecten gereduceerd worden? Om te onderzoeken of er bewust gestuurd kan worden, moet er eerst vastgesteld worden of er een relatie bestaat tussen factoren van trustworthiness en IT-outsourcing risico's (ITO-risico's).

In dit onderzoek wordt antwoord gegeven op de bovenstaande vragen. Middels een beperkt literatuuronderzoek, waarbij 27 artikelen zijn onderzocht, is er inzicht verkregen in de relatie tussen trustworthiness, IT-outsourcing en de risico's van IT-outsourcing. In het literatuuronderzoek heeft de onderzoeker twaalf ITO-risico's, die mogelijk verband houden met één of meerdere factoren van trustworthiness, geselecteerd op basis van literatuur en eigen interpretatie. In het empirisch onderzoek is onderzocht of deze twaalf ITO-risico's daadwerkelijk een relatie hebben met de factoren van trustworthiness en hoe sterk deze relatie het totaal aan vertrouwen beïnvloedt. De factoren van trustworthiness, benoemd door Mayer, zijn hiervoor gebruikt: ability, benevolence en integrity. Ability is de perceptie van vertrouwensgever over de groep van vaardigheden, competenties en karakteristieken van de vertrouwende partij, die het mogelijk maakt invloed uit te oefenen in een specifiek domein. Integrity is de perceptie van de vertrouwensgever dat de vertrouwde persoon een set van principes aanhoudt die voor vertrouwensgever acceptabel zijn. Benevolence wordt gedefinieerd als de mate waarin van een vertrouwde persoon geloofd wordt dat hij het beste voor heeft met de vertrouwensgever (Mayer, 1995). Middels interviews met respondenten is de relatie tussen de factoren van trustworthiness en ITO-risico's bevraagd. De respondenten hebben middels een Likertschaal aangegeven of zij een relatie zagen tussen de factoren en het ITO-risico. Daarnaast hebben zij een rapportcijfer gegeven over de invloed die deze relatie heeft op het totaal aan vertrouwen. Deze resultaten zijn verwerkt en geanalyseerd.

Uit dit onderzoek kan geconcludeerd worden dat alle ITO-risico's, die de onderzoeker vooraf heeft geselecteerd, een relatie hebben met één of meerdere factoren van trustworthiness. Daarbij is een conclusie dat hoe hoger de Likertwaarde, hoe hoger de beïnvloeding is van deze relatie op het totaal aan vertrouwen.

Summary

“The best way to find out if you can trust somebody is to trust them.”

- Ernest Hemingway

Trust is a well-researched subject within the social en psychological science. Even in business like behaviour one is attempted to explain more and more by meaning of trust (Earle, 2010). But what is trust and how is this measured? Can you willingly steer trustworthiness and can you reduce the perception of the defined risks within the IT-outsourcing trajectories? To investigate whether you can steer it willingly, you first have to determine if there is a relation between the factors of trustworthiness and the IT-outsourcing risks (ITO-risks).

In this study these questions will be answered. By means of a limited literary study, in which 27 articles were investigated, insight is given in the relation between trustworthiness, IT-outsourcing and the risks of IT-outsourcing. In this literary study, the investigator has selected twelve ITO-risks, risks which are possibly linked to one or more factors of trustworthiness. These twelve risks were selected from literature and own interpretation. In this empirical study these twelve ITO-risks were investigated whether they truly have a relation with the factors of trustworthiness and how strongly this relation influences the total amount of trust. The factors of trustworthiness are, according to Mayer, ability, benevolence and integrity. Ability is the perception of the trust giver about the group of skills, competences and characteristics from the trust receiver, which makes it possible to exercise influence within a specific domain. Integrity is the perception of the trust giver that the trust receiver upholds a set of principals which are acceptable to the trust giver. Benevolence is best defined as the extent to which a trust receiver is being believed when it comes to having the trust giver's best interest at heart.

By means of interviews with respondents the relation between the factors of trustworthiness and the ITO-risks was questioned. The respondents had to indicate by means of a Likertscale whether they saw a relation between the factors and the ITO-risk. Furthermore, the respondents also had to grade the influence of the relation on the total amount of trust. These result were processed and analysed.

From this study it can be concluded that all ITO-risks, which were selected upfront by the investigator, all have a relation with one or more factors of trustworthiness. The conclusion is that the higher the Likertscale, the higher the influence is on the total amount of trust in this relationship.

Inhoudsopgave

1	Introductie	8
1.1	Inleiding.....	8
1.1.1	Leeswijzer	8
1.2	Context.....	9
1.3	Relevantie	10
1.3.1	Praktische relevantie.....	10
1.3.2	Wetenschappelijke relevantie.....	10
1.4	Vraagstelling.....	11
1.5	Opdrachtformulering	11
2	Literatuurstudie	12
2.1	Doel en opzet	12
2.1.1	Onderzoeksvraag literatuuronderzoek	12
2.1.2	Zoekstrategie en uitvoering literatuuronderzoek	13
2.2	Resultaten en conclusies	14
2.2.1	Resultaten	14
2.2.2	Conclusies en vooruitblik voor het empirisch onderzoek	17
3	Doel van het empirisch onderzoek	17
3.1	Conceptueel onderzoeksmodel	18
4	Methode	19
4.1	Onderzoeksaanpak.....	19
4.2	Onderzoeksstrategie	19
4.2.1	Onderzoeksbenadering	19
4.2.2	Onderzoeksdoel	20
4.2.3	Onderzoeksmethoden.....	21
4.2.4	Tijdshorizon	21
4.2.5	Methode van gegevensverzameling	21
4.2.6	Primaire gegevensverzameling	22
4.2.7	Onderzoekspopulatie	22
4.2.8	Toegang tot respondenten, data en onderzoeksethiek	23
4.3	Aanpak en verzameling van gegevens	23
4.3.1	Vastlegging gegevens	23

Relation between factors of trustworthiness and IT-outsourcing risks: What is the influence of these relations on trust?

4.3.2	Werkwijze interviews	23
4.3.3	Gebruikte meetwaarden	24
4.3.4	Gebruikte software	26
4.4	Verwerking en analyse van de gegevens	26
4.4.1	Verwerking	26
4.4.2	Analyse en visualisatie	26
4.5	Validiteit en betrouwbaarheid	27
4.5.1	Betrouwbaarheid	27
4.5.2	Validiteit	27
4.5.3	Generaliseerbaarheid	28
4.6	Vooruitblik op resultaat	28
5	Uitvoering	28
6	Resultaten	30
6.1	Verzamelde gegevens	30
6.2	Verwerking van de gegevens	32
6.3	Analyse van de gegevens	33
6.3.1	Analyse van de gegevens voor onderzoeksvraag één	33
6.3.2	Analyse van de gegevens voor onderzoeksvraag twee	38
7	Conclusies en aanbevelingen	43
7.1	Conclusies	43
7.2	Aanbevelingen voor verder onderzoek	45
8	Reflectie	45
8.1	Kwaliteit onderzoeksdata en houdbaarheid van de conclusies	45
9	Dankwoord	47
10	Referenties	48
11	Appendices	50
11.1	Appendix 1: Begrippenlijst	50
11.2	Appendix 2: Literatuurstudierapport	54
11.3	Appendix 3: Motivering onderzoeksmethode	106
11.4	Appendix 4: Gegevensverzamelingsformulier	108
11.5	Appendix 5: Draaiboek interviews	109
11.6	Appendix 6: Begrippen onderzoek en interviews	111
11.7	Appendix 7: Gegevensverzameling per respondent	116
11.7.1	Respondent 1	116
11.7.2	Respondent 2	123
11.7.3	Respondent 3	128

Relation between factors of trustworthiness and IT-outsourcing risks: What is the influence of these relations on trust?

11.7.4	Respondent 4.....	135
11.8	Appendix 8: Transcriptie interviews per respondent.....	136
11.8.1	Respondent 1.....	136
11.8.2	Respondent 2.....	148
11.8.3	Respondent 3.....	155
11.9	Appendix 9: Overzicht van de afwijkingen van de beïnvloeding van de relatie.....	162
11.10	Appendix 10: Percentages Likertwaarden per relatie	165

1 Introductie

1.1 Inleiding

De afgelopen 25 jaar heeft outsourcing van Informatie Technologie (IT) een enorme vlucht genomen. Waar eerst alles 'in huis' werd gehouden, worden nu steeds meer delen van de bedrijfsvoering uitbesteed aan andere organisaties die in die desbetreffende werkzaamheden gespecialiseerd zijn (Langfield-Smith, 2001).

In het uitbesteden van kritieke IT-systemen van je onderneming creëert men een grote afhankelijkheid. Wat gebeurt er als het mis gaat, wat betekent dit voor de continuïteit, beschikbaarheid en integriteit van de gegevens, en de informatiesystemen van de onderneming? Het uitbesteden van (delen van) IT brengt voordelen, nadelen en risico's met zich mee. Bij het uitbesteden van IT neemt men dus risico's, waarbij de kans dat ze ontstaan zo laag mogelijk gehouden moet worden en waarbij de impact van de risico's tevens zo laag mogelijk gehouden moet worden. Hiervoor zullen maatregelen genomen moeten worden.

Daarnaast wordt steeds meer getracht om het zakelijk gedrag te verklaren middels vertrouwen (Earle, 2004). Hierbij rijst de vraag of factoren van *trustworthiness* als stuurmiddel gebruikt kunnen worden om de perceptie van IT-outsourcing risico's te reduceren.

Uit onderzoek naar kenmerken van relaties en hun invloed op het succes van outsourcing blijkt dat bepaalde relationele kenmerken (bijvoorbeeld: de volledigheid van het formele contract, de perceptie van de kwaliteit van de dienstverlening, vertrouwen en flexibiliteit) positief correleren met het succes van outsourcing. Vandaar dat naast de strategische beslissing van wat er uitbesteed zal worden, de operationele sturing van deze relationele kenmerken ervoor kunnen zorgen dat het outsourcing traject een succes wordt (Urbach & Wurz, 2012).

Een van de kenmerken van relaties is dat er een zekere mate van vertrouwen tussen partijen bestaat of ontstaat. Hoe hoog dit vertrouwen is hangt af van bepaalde elementen, waaronder factoren van *trustworthiness*. De factoren van *trustworthiness* worden door Mayer gedefinieerd als *ability* (bekwaamheid), *benevolence* (welwillendheid) en *integrity* (integriteit) (Mayer, 1995). Aangezien de mate van vertrouwen afhangt van deze factoren rijst de vraag of er bewust gestuurd kan worden op deze factoren om zodoende het vertrouwen te verhogen?

Dit onderzoek richt zich op de vraag of er gestuurd kan worden in het zakelijk gedrag, door te sturen op vertrouwen, binnen een IT-outsourcing traject.

1.1.1 Leeswijzer

Voor de leesbaarheid van dit document is de begrippenlijst opgenomen in appendix 1.

Dit document is als volgt opgebouwd:

- Hoofdstuk één bevat de context waarbinnen dit onderzoek is uitgevoerd, de probleemstelling, de relevantie van dit onderzoek en de uiteindelijke opdrachtformulering;
- Hoofdstuk twee bevat voor het empirisch onderzoek relevante delen van het literatuuronderzoek;
- Hoofdstuk drie bevat het doel van het empirisch onderzoek en het conceptueel onderzoeksmodel;
- Hoofdstuk vier bevat de aanpak van onderzoek, waaronder de onderzoeksmethode, onderzoeksstrategie, aanpak en verzameling van gegevens, verwerking en analyse van de gegevens, validiteit en betrouwbaarheid en een vooruitblik op de uitvoering van het

- onderzoek;
- Hoofdstuk vijf bevat de uitvoering van het empirisch onderzoek;
- Hoofdstuk zes bevat de resultaten van het empirisch onderzoek, de verwerking van de verzamelde gegevens en de analyse van de verzamelde gegevens;
- Hoofdstuk zeven bevat de conclusies en de aanbevelingen. Hier staan de belangrijkste conclusies van het onderzoek en een aanzet voor vervolgonderzoek;
- Hoofdstuk acht bevat de reflectie op het onderzoek;
- Hoofdstuk negen bevat het dankwoord;
- Hoofdstuk tien bevat alle appendices.

1.2 Context

Dit onderzoek vindt plaats binnen het gebied van IT-outsourcing, risicomanagement en vertrouwen. Binnen deze gebieden wordt een aantal basisdefinities gebruikt die hieronder worden weergegeven.

Outsourcing wordt gedefinieerd als: het uitbesteden van een dienst of activiteit aan een derde partij (Langfield-Smith, 2001). Outsourcing wordt steeds meer toegepast, niet alleen voor de productieactiviteiten, maar ook steeds meer voor de traditionele in-house activiteiten zoals administratieve- en managementfuncties, inclusief de verwerking van gegevens en IT-activiteiten, human resource management services, accounting functies, interne audit en marketing (Chalos, 1995; Langfield-Smith, 2001).

De omvang en de kosten van de diensten en/of producten zijn voor veel organisaties van invloed om steeds meer gericht te zijn op de uitbesteding van deze diensten en/of producten. The Boston Consulting Group (1991) heeft onderzoek gedaan naar meer dan 100 belangrijke bedrijven met uitgebreide outsourcing en concludeerde dat de meeste westerse bedrijven in de eerste plaats uitbesteden om te besparen op *overhead* of induceren op korte termijn kostenbesparingen (Kadabade, 2000).

Het uitbesteden van diensten en/of producten wordt ook steeds vaker toegepast in de IT. Hier wordt het Information Technology Outsourcing (ITO) genoemd, wat er op neer komt dat alle IT-bezittingen, -resources en -activiteiten worden overgedragen aan een derde partij die zorg gaat dragen voor het beheer.

Normaal gesproken gaat er een heel proces aan vooraf, voordat er gekozen wordt voor een partij die voldoet aan de eisen van de klant. Hierbij hoort vaak ook een risicoanalyse, waarbij naast de risico's ook de voor- en nadelen worden beschreven van outsourcing van de IT (Aung, 2008; Kadabade, 2000). Deze risico's van de outsourcing van de IT zullen beheerd moeten worden binnen het risicomanagement.

De standaard van risicomanagement, ISO 31000, definieert risico management als *'gecoördineerde activiteiten om het risico van de organisatie te sturen en controleren, gedefinieerd als een combinatie van de gevolgen van een gebeurtenis en de bijbehorende kans. Het risico management proces wordt gedefinieerd als de systematische toepassing van het management beleid, de procedures, activiteiten met betrekking tot het communiceren, raadplegen, vaststellen van de context, en het identificeren, analyseren, evalueren, behandeling, monitoring, en reviewen van het risico'* (ISO Guide 73:2009, definitie 2.1).

In de definitie van risicomanagement zit tevens de definitie van risico: *risico is het effect van onzekerheid op het behalen van doelstellingen* (ISO Guide 73:2009, definitie 2.1).

Naast objectieve indicatoren bestaan er ook "zachtere" indicatoren waarop gestuurd kan worden tijdens de risicoanalyse. Vertrouwen is een van deze "zachtere" indicatoren die de laatste jaren

veelvuldig is onderzocht binnen diverse disciplines. Ook is vertrouwen (*trust*) een centraal begrip aan het worden in het verklaren van zakelijk gedrag in de organisatorische context (Earle, 2004).

In de literatuur wordt aan het woord 'vertrouwen' verschillende betekenissen gegeven. Zo is er ook in de Engelse taal een verschil in de vertaling van vertrouwen. Wat het verschil is tussen *confidence* en *trust*, en welke indicatoren daarbij horen wordt in het literatuuronderzoek verder uitgewerkt. In dit onderzoek wordt gesproken over trustworthiness. Google translate vertaalt dit als betrouwbaarheid, maar betrouwbaarheid wordt vertaald als *reliability* en deze term heeft een andere betekenis dan trustworthiness. Vertrouwenswaardig is een woord dat dicht in de buurt komt van een vertaling van trustworthiness, maar om het zuiver te houden zal de Engelse terminologie aangehouden worden.

1.3 Relevantie

1.3.1 Praktische relevantie

Indien vertrouwen als instrument ingezet kan worden om de perceptie van risico's te reduceren, kan dit in het voordeel werken voor zowel de uitbestedende als de leverende partij. Vertrouwen kan dan bewust beïnvloed worden door middel van de factoren van trustworthiness, om er als partij voordeel mee te doen; als leverancier om je trustworthiness te vergroten naar de klanten toe en als klant om een leverancier uit te zoeken op basis van de factoren van trustworthiness.

Om als leverende partij een klant binnen te halen en te binden kunnen er factoren die vertrouwen oproepen ingezet worden om invloed uit te oefenen op het risicomanagement van de klant. Dit kan door middel van verschillende factoren. Hiermee kan de leverancier zich focussen op de vraag: 'Hoe ben je een betrouwbare partner voor de klant?'

Als klant kun je binnen je risicomanagement de perceptie van de gedefinieerde risico's verminderen door te kijken naar leveranciers die je 'vertrouwt'. De klant kan op basis van de factoren van trustworthiness beoordelen of hij de leverancier vertrouwt, er vertrouwen bestaat tussen beide organisaties of eventueel zou kunnen ontstaan.

Voor zowel de uitbestedende als de leverende partij zullen inzichten in het bewust sturen middels vertrouwen, op de risico's van IT-outsourcing, leiden tot het beter en gefundeerd maken van zakelijke keuzes met betrekking tot het vinden van een juiste IT-partner.

1.3.2 Wetenschappelijke relevantie

In de literatuur is het bewust sturen van factoren van trustworthiness, om risico's te reduceren, nog onvoldoende onderzocht. Er is veel onderzocht met betrekking tot vertrouwen en risico management, maar binnen het literatuuronderzoek heeft de onderzoeker niets gevonden over het bewust sturen middels factoren van trustworthiness binnen het vakgebied organisatiemanagement. Onderzoek hiernaar zou een interessante aanvulling kunnen zijn op de bestaande literatuur met betrekking tot vertrouwen, IT-outsourcing en de risico's hiervan. Omdat 'vage' termen als vertrouwen of trustworthiness moeilijk objectief te meten zijn, is het interessant om te onderzoeken of er een relatie bestaat tussen vertrouwen en ITO-risico's. Met de uitkomsten hiervan kan vervolgens onderzocht worden welke factoren een bepaalde invloed hebben om hier vervolgens bewust op te sturen. Indien bewust gestuurd kan worden op factoren van trustworthiness ontstaan er meer inzichten in de werking tussen sociale psychologische componenten en het maken van zakelijke keuzes.

1.4 Vraagstelling

Vertrouwen is iets dat bestaat tussen twee of meerdere personen. Echter, omdat het een gevoelskwestie betreft is het vertrouwen van de ene persoon niet identiek aan het vertrouwen van de andere persoon. Vertrouwen is een subjectief begrip, maar toch hebben onderzoekers in zowel de sociale- als psychologische hoek getracht dit te onderzoeken aan de hand van indicatoren (Earle, 2004, 2010; Gill, 2005).

Uit de literatuur blijkt dat de factoren van trustworthiness correleren met hoe betrouwbaar iemand gevonden wordt (Gill, 2005). Daarnaast wordt gesteld dat hoe hoger het vertrouwen, hoe lager de perceptie van de gedefinieerde risico's is (Nooteboom, 2000).

Bij outsourcing van IT komen diverse risico's naar voren waarvan de perceptie zo laag mogelijk gehouden moet worden. Kan door het beïnvloeden van factoren van trustworthiness de perceptie van gedefinieerde risico's bijgesteld worden? Dat beïnvloeden gebeurt al dan niet bewust. Maar kan hier dan ook op gestuurd worden en kunnen deze factoren bewust beïnvloed worden? Hoe kan door het bewust beïnvloeden van de factoren van trustworthiness de perceptie van gedefinieerde risico's gereduceerd worden?

1.5 Opdrachtformulering

Zoals in de inleiding al benoemd is wordt zakelijk gedrag steeds meer getracht te verklaren middels vertrouwen. Daarbij rijst de vraag of er dan ook gestuurd zou kunnen worden in het zakelijk gedrag door middel van beïnvloeding van factoren van trustworthiness. Oftewel, hoe kan de perceptie van de risico's, gedefinieerd binnen je risicomanagement, gereduceerd worden door te sturen middels factoren van trustworthiness?

Vanuit de vraagstelling komt naar voren of er bewust gestuurd kan worden op de factoren van trustworthiness om zodoende de perceptie van de ITO-risico's te verlagen.

In de literatuur komt naar voren dat indien het vertrouwen tussen partijen hoog is, de risico's lager worden ingeschat (Das, 2001). Vanuit de probleemstelling en de relevantie kan de onderstaande hoofdvraag van het theoretische onderzoek, het literatuuronderzoek, beschreven worden:

“Hoe kunnen factoren van vertrouwen bewust ingezet worden om de perceptie van de risico's van IT-outsourcing te verlagen?”

Als de perceptie van het risico lager is, wordt de kans dat het risico zich voordoet lager ingeschat. De kans wordt hiermee dus lager en de impact ook, aangezien het effect niet kan veranderen ($\text{impact} = \text{kans} * \text{effect}$). Het effect kan niet veranderen omdat de gevolgen van een risico vaststaan. Bijvoorbeeld: er bestaat een risico dat bij hoog water de dijk overstroomt. Indien het risico zich voordoet, zal ook daadwerkelijk de dijk overstromen. Aan de kans dat dit zich voordoet kan iets veranderd worden, namelijk de dijk wordt hoger gemaakt. Aan het gevolg (dus het effect) van het risico kan niets veranderd worden. De inschatting van de kans is altijd een perceptie van een persoon.

Kunnen factoren van trustworthiness bewust ingezet worden om de perceptie van gedefinieerde risico's te reduceren binnen je risicomanagement bij outsourcing van IT, met als doel om hierop te sturen?

Uit het literatuuronderzoek is hier geen duidelijk antwoord op gevonden. Wel zijn er door de onderzoeker IT-outsourcing risico's gedefinieerd die samenhangen met vertrouwen. In het literatuuronderzoek heeft de onderzoeker de factoren van trustworthiness aan de IT-outsourcing risico's gekoppeld, met gebruik van eigen interpretatie. In het empirisch onderzoek gaat de

onderzoeker vaststellen of deze factoren van trustworthiness in relatie te brengen zijn met de ITO-risico's, en ook in welke mate deze relatie de perceptie van het totaal aan vertrouwen beïnvloedt.

Naar aanleiding van het literatuuronderzoek en de gevonden informatie is de onderzoeksvraag aangepast en in twee delen opgesplitst.

De aangescherpte onderzoeksvragen luiden:

- 1. In hoeverre bestaat er een invloed van één of meerdere factoren van trustworthiness op de perceptie van IT-outsourcing risico's?**
- 2. Indien er invloed is op de perceptie van ITO-risico's, hoe sterk is deze invloed?**

Onderzoeksvraag twee is geen vraag die op zichzelf staand is, omdat deze vraag een andere onderzoekstrategie vereist, die buiten de scope van dit onderzoek ligt. De informatie die met onderzoeksvraag twee wordt beoogd te verkrijgen kan input leveren voor eventueel vervolgonderzoek naar de invloed die de factoren van trustworthiness hebben op ITO-risico's en hoe hierop gestuurd kan worden. Vanuit een vervolgonderzoek gebaseerd op deze input zouden de vragen die in de vraagstelling, paragraaf 1.4, beantwoord kunnen worden.

2 Literatuurstudie

Vertrouwen is een veel onderzocht onderwerp binnen de sociale - en psychologische wetenschap (Davis, 1999; Earle, 2004, 2010; Mayer, 1995). Ook zakelijk gedrag wordt steeds meer getracht te verklaren door middel van vertrouwen (Earle, 2004). Wat zijn factoren van vertrouwen en hoe worden deze gemeten? Vanuit de zakelijke hoek is het interessant om te kijken of er bewust middels factoren van trustworthiness op ITO-risico's gestuurd kan worden. Kan de perceptie van gedefinieerde risico's binnen IT-outsourcing hiermee gereduceerd worden?

In het literatuuronderzoek wordt antwoord gegeven op de bovenstaande vragen. Middels een beperkt literatuuronderzoek, waarbij 27 artikelen zijn onderzocht, is er inzicht gegeven in de relatie tussen vertrouwen, IT-outsourcing en de risico's van IT-outsourcing.

Een voorlopige conclusie is dat, door middel van beïnvloeding van de drie factoren van trustworthiness: integriteit, welwillendheid en bekwaamheid, benoemd door Mayer, de perceptie van trustworthiness van een partij vergroot kan worden. Dit geldt zowel vanuit de klantzijde als vanuit de leverancierszijde.

Tevens is een belangrijke conclusie dat er binnen de literatuur veel is onderzocht met betrekking tot vertrouwen en risico management, maar dat de onderzoeker binnen het literatuuronderzoek niets heeft gevonden over het *bewust* sturen middels factoren van trustworthiness. Omdat de onderzoeker het bewust sturen van factoren van trustworthiness niet heeft kunnen blootleggen binnen het literatuuronderzoek, is dit een aanleiding om dit onderwerp door de onderzoeker in een empirisch onderzoek nader te verkennen.

De belangrijkste punten voor het literatuuronderzoek zijn in dit hoofdstuk beschreven. De onderzochte literatuur die niet als afzonderlijk is benoemd in dit hoofdstuk, zal in de conclusies van het literatuuronderzoek kort aangestipt worden. Het volledige literatuuronderzoek is als appendix 2 toegevoegd aan dit rapport.

2.1 Doel en opzet

2.1.1 Onderzoeksvraag literatuuronderzoek

Vanuit de probleemstelling en de relevantie, zoals benoemd in het literatuuronderzoek in appendix 2, kan de onderstaande hoofdvraag van dit theoretische onderzoek beschreven worden:

Hoe kunnen factoren van vertrouwen bewust ingezet worden om de perceptie van de risico's van IT-outsourcing te verlagen?

Voor het opbouwen van het theoretisch kader is een aantal onderzoeksvragen geformuleerd. Deze onderzoeksvragen zijn opgesteld om een antwoord te krijgen op de context van het onderzoek en op de hoofdvraag.

1. *Wat wordt verstaan onder vertrouwen?*
2. *Welke relaties bestaan er tussen organisaties?*
3. *Wat wordt verstaan onder risicomanagement?*
4. *Wat zijn de risico's bij outsourcing van IT?*
5. *Welke rol speelt vertrouwen bij vastlegging van afspraken tussen partijen?*
6. *Welke indicatoren van vertrouwen bestaan er vanuit de literatuur?*
7. *Is er een verband tussen risicomanagement en vertrouwen?*
8. *Op welke manier kan vertrouwen ingezet worden en hoe kan dit gemeten worden binnen IT-outsourcing?*

2.1.2 Zoekstrategie en uitvoering literatuuronderzoek

Voor het literatuuronderzoek is gebruik gemaakt van de literatuurbronnen zoals deze aangeboden worden op de "Digitale Bibliotheek" van de Open Universiteit. Hierbij is gezocht binnen alle disciplines, omdat het begrip "Vertrouwen" verder rijkt dan de discipline "managementwetenschappen".

Om een zo scherp mogelijke set van artikelen te verkrijgen zijn onderstaande keywords (Engels en Nederlands) samengesteld waarop is gezocht:

- riskmanagement / risicomanagement;
- trust, confidence/ vertrouwen;
- trustworthiness / betrouwbaarheid;
- factors / factoren;
- antecedents;
- organizational trust / organisatie vertrouwen;
- organisational trust / organisatie vertrouwen;
- relationship / relatie;
- organisation / organisatie;
- organization / organisatie;
- business / bedrijf;
- IT-outsourcing;
- risks / risico's;
- control / sturen;
- steer / sturen;
- definition / definitie;
- contract.

In hoofdstuk 3 van het literatuuronderzoek zijn de samengestelde query's opgenomen, waarop per onderzoeksvraag is gezocht, zie appendix 2.

Aanvullende opmerkingen:

- De genoemde keywords zijn zowel zelfstandig (bijvoorbeeld Trust) als in combinatie met elkaar gebruikt (bijvoorbeeld Trust + organisation);

- Bij dit literatuuronderzoek is er voornamelijk gezocht naar Engelstalige literatuur en in beperkte mate naar Nederlandstalige literatuur;
- Bij het selecteren van de keywords is rekening gehouden met zowel de Britse als de Amerikaanse spelling;
- Bij het zoeken naar literatuur is niet ingeperkt op datum van publicatie;
- De resultaten van de literatuurstudie zijn beheerd met behulp van EndNote, bibliografische software van Reuters;
- In de uitwerking van dit onderzoek zullen Engelse kreten en terminologie gebruikt worden aangezien er in het Nederlands niet altijd de juiste vertaling voor te vinden is.

Tijdens de oriëntatie naar het onderzoeksonderwerp zijn er twee belangrijke review artikelen naar voren gekomen. Aan de hand van deze twee artikelen is de sneeuwbalmethode toegepast om te zoeken naar artikelen waarna gerefereerd wordt in de teksten. De sneeuwbalmethode is tevens toegepast op andere relevante artikelen.

2.2 Resultaten en conclusies

In deze paragraaf worden de belangrijkste resultaten en conclusies weergegeven. Voor de volledige resultaten en conclusies wordt verwezen naar het rapport van het literatuuronderzoek, welke als appendix 2 is toegevoegd bij dit rapport.

2.2.1 Resultaten

2.2.1.1 Vertrouwen

In de literatuur zijn vele definities van vertrouwen te vinden. In dit onderzoek wordt onderstaande definitie van Mayer (1995) gehanteerd, aangezien naar deze definitie in vele onderzoeken wordt verwezen en breed wordt gedragen binnen de literatuur (Rousseau, Sitkin, Burt, & Camerer, 1998).

“Vertrouwen is een psychologische toestand die de kwetsbaarheid accepteert op basis van positieve verwachtingen van de intenties of het gedrag van een ander” (Mayer, 1995).

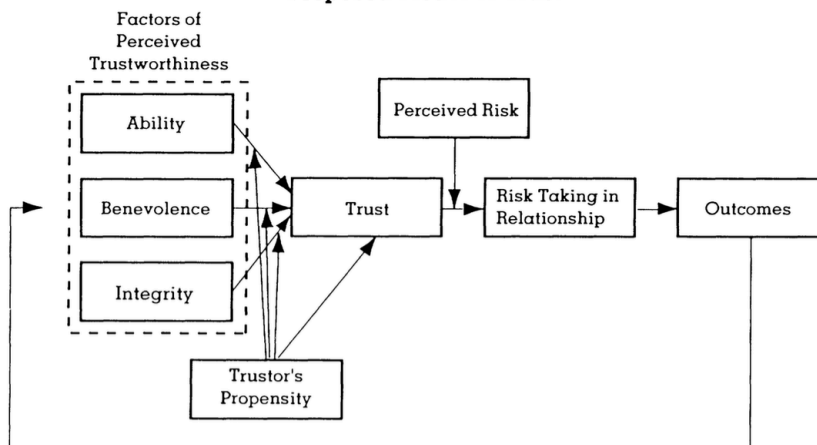
Tortoriello ontleedt deze definitie en stelt dat in deze definitie twee elementen zitten (Bill McEvily, 2011):

1. De bereidheid om kwetsbaar te zijn;
2. De verwachting van een gunstige behandeling door een andere partij.

Mayer stelt dat er in deze definitie van vertrouwen de bereidheid zit om risico's te nemen en kwetsbaar te zijn. Volgens Mayer is dit in deze definitie de belangrijkste factor (Mayer, 1995). Indien er geen risico's zijn om te accepteren ontstaat er ook niets om te vertrouwen.

Mayer heeft een model ontwikkeld waarbij de concentratie ligt op het vertrouwen in een organisatorische setting waarbij twee specifieke partijen deelnemen: een vertrouwende partij (*trustor*) en een partij te vertrouwen (*trustee*).

FIGURE 1
Proposed Model of Trust



Figuur 1: Model of Trust (Mayer, 1995)

In het model van Mayer wordt risico gescheiden van het vertrouwen. Vertrouwen brengt niet per se risico met zich mee, maar een bereidheid om een risicovolle relatie aan te gaan met de trustee, bijvoorbeeld: het delen van vertrouwelijke informatie (Gill, 2005).

Dit model past daarmee perfect op de onderzoeksvraag. Als er in Figuur 1 meer trust is, zal het 'perceived risk' lager zijn. De 'factors of perceived trustworthiness' zijn dus mogelijk belangrijke input- c.q. stuurfactoren voor het verlagen van het gepercipieerde risico.

Mayer definieert drie factoren die ook in het Model of Trust benoemd zijn:

- *ability* (bekwaamheid, kundigheid);
- *benevolence* (welwillendheid);
- *integrity* (integriteit).

Ability is de perceptie van vertrouwensgever over de groep van vaardigheden, competenties en karakteristieken van de vertrouwende partij, die het mogelijk maken invloed uit te oefenen in een specifiek domein. Integrity is de perceptie van de vertrouwensgever dat de vertrouwde persoon een set van principes aanhoudt die voor vertrouwensgever acceptabel zijn. Benevolence wordt gedefinieerd als de mate waarin van een vertrouwde persoon geloofd wordt dat hij het beste voorheeft met de vertrouwensgever (Mayer, 1995).

Als set lijken deze drie een groot deel van trustworthiness te verklaren. Elk van deze drie draagt bij aan een uniek perspectief van vertrouwen, terwijl alle drie samen een solide en spaarzaam fundament biedt voor de empirische studie van vertrouwen voor een andere partij (Mayer, 1995).

2.2.1.2 Wat zijn de risico's bij outsourcing van IT?

Om te onderzoeken of factoren van vertrouwen bewust ingezet kunnen worden om de perceptie van ITO-risico's te verlagen is het nodig om een lijst samen te stellen met ITO-risico's. Hiervoor heeft de onderzoeker een literatuuronderzoek gebruikt van J. Tetteroo. J. Tetteroo heeft uitvoerig onderzoek gedaan naar risico's binnen IT-outsourcing. In zijn literatuuronderzoek heeft hij een overzicht gemaakt, waarin hij 38 ITO-risico's benoemt (Tetteroo, 2016).

Deze lijst met ITO-risico's van Tetteroo is in het literatuuronderzoek opgenomen, zie hiervoor appendix 2.

2.2.1.3 Risico's van IT-outsourcing die verband houden met trustworthiness

Uit onderzoek naar kenmerken van relaties en hun invloed op het succes van outsourcing, blijkt dat bepaalde relationele kenmerken (bijvoorbeeld, de volledigheid van het formele contract, de perceptie van de kwaliteit van de dienstverlening, vertrouwen en flexibiliteit) positief correleren met het succes van outsourcing. Vandaar dat naast de strategische beslissing van wat er uitbesteed zal worden, de operationele sturing van deze relationele kenmerken ervoor kan zorgen dat het outsourcing traject een succes wordt (Urbach & Wurz, 2012).

Tijdens een outsourcing traject moet regie worden gehouden op de IT-leverancier en de governance geborgd zijn. Om te sturen op de IT-leverancier zijn er objectieve indicatoren, zoals contracten, service levels, etc. Naast deze objectieve indicatoren bestaan er ook "zachtere" indicatoren waarop gestuurd zou kunnen worden. Deze zachtere indicatoren kunnen onder andere factoren van trustworthiness zijn.

In het literatuuronderzoek is enerzijds een lijst met risico's van IT-outsourcing benoemd en zijn anderzijds factoren van trustworthiness benoemd. Om een verband te leggen tussen de risico's van IT-outsourcing en de factoren van trustworthiness heeft de onderzoeker getracht om deze bij elkaar te brengen door middel van eigen interpretatie, gebaseerd op literatuur.

Aan de hand van de gedefinieerde risico's van IT-outsourcing is door de onderzoeker geïnventariseerd welke ITO-risico's een verband hebben met vertrouwen. Van de 38 risico's benoemd door J. Tetteroo, lijken er twaalf beïnvloedbaar te zijn via de factoren van trustworthiness.

Daarbij is tevens gekeken naar welke factor van trustworthiness (integrity, benevolence, ability (Mayer, 1995)) dit risico mogelijk beïnvloedt. Deze is in de vierde kolom van Tabel 1 weergegeven.

De drie factoren die Mayer benoemt, die te maken hebben met trustworthiness, heeft de onderzoeker naast de risico's van IT-outsourcing gelegd. Hierdoor blijft een lijst over van ITO-risico's die specifiek gericht zijn op de factoren van trustworthiness. Deze lijst is gebaseerd op de interpretatie van de onderzoeker. Om de keuzes inzichtelijk te maken is deze interpretatie in het literatuuronderzoek als bijlage opgenomen.

Dit bij elkaar brengen van de IT-outsourcing risico's en de factoren van trustworthiness heeft geresulteerd in onderstaande Tabel 1, met twaalf ITO-risico's.

Tabel 1: ITO-risico's met betrekking tot vertrouwen samengesteld door de onderzoeker

#	ITO Risico's (Tetteroo, 2016)	Factor van vertrouwen
1	Backlash from internal IT staff	Integrity
2	Contractual risk	Integrity, benevolence, ability
3	Coordination between client and supplier	Integrity, benevolence, ability
4	Cultural differences between client and supplier	Integrity, benevolence
5	Difficulty in managing remote teams	Integrity, benevolence
6	Lack of trust	Integrity, benevolence, ability
7	Loss of control over data	Integrity, ability
8	Opportunistic behaviour	Integrity, benevolence

9	Security / privacy breach	Integrity
10	Shirking	Integrity
11	Single / Double moral hazard	Integrity
12	Supplier employees have poor communication skills	Benevolence

2.2.2 Conclusies en vooruitblik voor het empirisch onderzoek

Er is veel binnen de literatuur onderzocht met betrekking tot vertrouwen en risico management, maar binnen het literatuuronderzoek heeft de onderzoeker niets gevonden over het bewust sturen van factoren van trustworthiness op ITO-risico's om de perceptie hiervan te verlagen. Dat er niets is gevonden door de onderzoeker is een reden om te onderzoeken of deze vraag relevant is. Om relevant materiaal te verzamelen voor vervolgonderzoek is het noodzakelijk om eerst te onderzoeken of de factoren van trustworthiness invloed hebben op ITO-risico's. En indien één of meerdere factoren invloed hebben op ITO-risico's hoe groot is deze invloed dan op het totaal aan vertrouwen.

In het literatuuronderzoek zijn de factoren van trustworthiness van Mayer hiervoor geselecteerd. Hebben deze factoren van trustworthiness invloed op ITO-risico's? Middels een empirisch onderzoek wordt er eerst vastgesteld of de factoren van trustworthiness daadwerkelijk invloed hebben op de geselecteerde IT-outsourcing risico's. Dit vervolgonderzoek wordt verder uitgewerkt in hoofdstuk 3 en 4.

3 Doel van het empirisch onderzoek

Omdat 'vage' onderwerpen zoals vertrouwen moeilijk meetbaar zijn, is er al lange tijd behoefte voor een meetinstrument die 'objectief' het vertrouwen kan meten en waarbij het onderzoek ook replicerbaar is.

Uit de resultaten van het literatuuronderzoek komt naar voren dat vertrouwen moeilijk meetbaar is. Er is geen meetinstrument waarmee vertrouwen objectief gemeten kan worden binnen het *vakgebied organisatie vertrouwen* en specifiek binnen IT-outsourcing. Binnen het *vakgebied vertrouwen in risicomanagement* bestaat wel een meetinstrument, namelijk het consensus model van Earle (2010).

De onderzoeksvraag van het literatuuronderzoek was geformuleerd als:

"Hoe kunnen factoren van vertrouwen bewust ingezet worden om de perceptie van de risico's van IT-outsourcing te verlagen?"

Om vertrouwen te meten en eventueel bewust mee te sturen vanuit het risicomanagement, is het allereerst noodzaak om te weten of er een relatie bestaat tussen vertrouwen en ITO-risico's. Oftewel, hebben de factoren van trustworthiness invloed op ITO-risico's? Indien deze factoren invloed hebben op de ITO-risico's moet er vervolgens onderzocht worden hoe groot deze invloed is.

Gedurende het literatuuronderzoek heeft de onderzoeker al een voorzet genomen en de relevante ITO-risico's gekoppeld aan de factoren van trustworthiness van Mayer. Middels het empirisch onderzoek wordt er getoetst of de factoren van trustworthiness daadwerkelijk invloed hebben op ITO-risico's en hoe groot deze invloed is.

Naar aanleiding van het literatuuronderzoek is daarom de onderzoeksvraag aangescherpt en in twee delen opgesplitst.

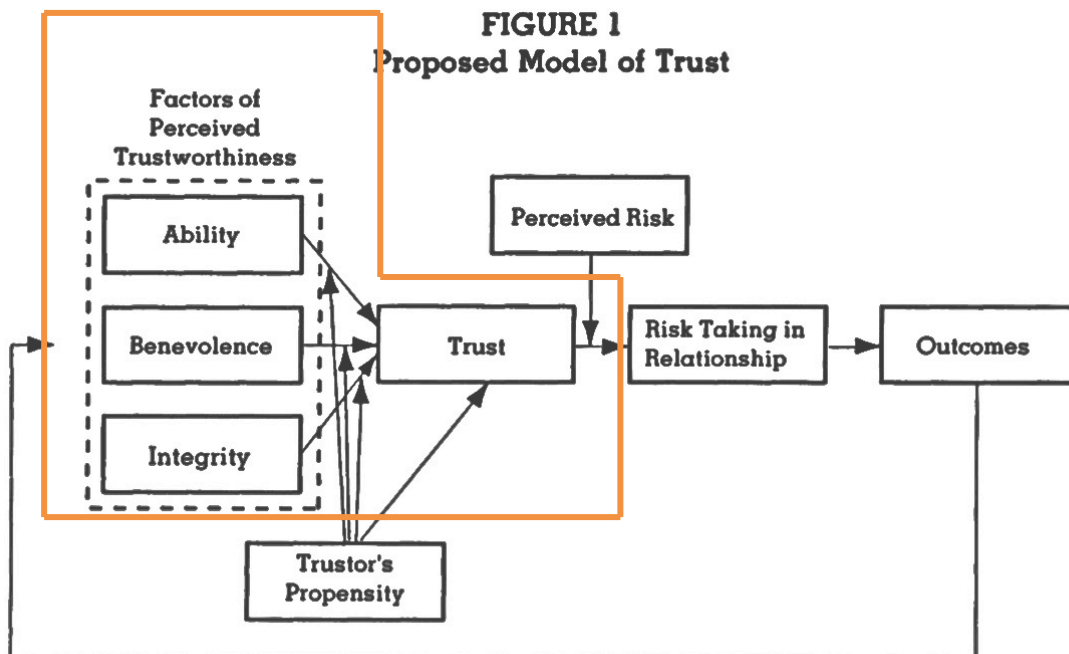
De aangescherpte onderzoeksvragen luiden:

1. In hoeverre bestaat er een invloed van één of meerdere factoren van trustworthiness op de perceptie van IT-outsourcing risico's?
2. Indien er invloed is op de perceptie van ITO-risico's, hoe sterk is deze invloed?

Het empirisch onderzoek zal antwoord geven op bovenstaande vragen. Daarbij wordt gezocht naar een relatie tussen de factoren van trustworthiness en ITO-risico's. Dit wordt ook zo verwoord in deze scriptie. Daar waar gesproken wordt over een relatie tussen deze factoren en ITO-risico's wordt bedoeld dat de factoren van trustworthiness een invloed hebben op de perceptie van ITO-risico's. Dit onderzoek heeft als doel om als input te dienen voor een eventueel vervolgonderzoek. Dit vervolgonderzoek zou de initiële onderzoeksvraag van het literatuuronderzoek kunnen beantwoorden; *"hoe kunnen factoren van vertrouwen bewust ingezet worden om de perceptie van de risico's van IT-outsourcing te verlagen?"*

3.1 Conceptueel onderzoeksmodel

Om de onderzoeksvragen van het empirisch onderzoek te beantwoorden wordt er gebruik gemaakt van een conceptueel onderzoeksmodel. Het model dat hiervoor gebruikt wordt is het Model of Trust van Mayer (1995), zie Figuur 1. De onderzoeker gebruikt echter slechts een deel van dit model, omdat de onderzoeker op zoek gaat naar een relatie tussen de factoren van trustworthiness en ITO-risico's. Derhalve gebruikt de onderzoeker alleen de begrippen van trustworthiness uit het Model of Trust van Mayer. Perceived Risk, Risk Taking in Relationship, Outcomes en Trustor's Propensity vallen niet binnen de scope van het empirisch onderzoek. Het deel dat de onderzoeker gebruikt valt in het model binnen de rode lijnen.



Figuur 1: Model of Trust (Mayer, 1995)

4 Methode

4.1 Onderzoeksaanpak

In deze paragraaf zal in grote lijnen de aanpak van het onderzoek beschreven worden. De ontwerpbeslissingen worden in de rest van het hoofdstuk nader toegelicht en onderbouwd.

De combinatie van vertrouwen en ITO-risico's moet voortkomen uit interviews met de doelgroep. De methode van gegevensverzameling wordt in paragraaf 4.2.5 nader onderbouwd en de doelgroep wordt in paragraaf 4.2.7. nader toegelicht. Er zal aan respondenten gevraagd worden welke factoren van trustworthiness van invloed zijn op het desbetreffende ITO-risico.

In het tweede deel van het empirisch onderzoek wordt getoetst hoe groot de invloed is van de drie factoren van trustworthiness op de totale hoogte van de perceptie van het ITO-risico. Hierbij wordt vastgesteld, aan de hand van de interviews met de respondenten, wat de verschillende factoren van trustworthiness voor een invloed hebben op de ITO-risico's. Met andere woorden: wat gebeurt er met de perceptie van de hoogte van de ITO-risico's indien er op een bepaalde factor meer of minder wordt gescoord? Dit wordt vastgesteld door de input te voorzien van een cijfer per relatie. Deze meetwaarde wordt in paragraaf 4.3.3. nader toegelicht.

Indien er een correlatie bestaat tussen de factoren van trustworthiness en de ITO-risico's zou hierop bewust gestuurd kunnen worden, omdat impact en resultaat van acties hiermee inzichtelijk kunnen worden gemaakt. Indien er meer geïnvesteerd wordt in een bepaalde factor van trustworthiness kan dit impact hebben op het totaal aan vertrouwen.

Om het empirisch onderzoek grondig en gestructureerd te laten verlopen zal er een aantal stappen genomen worden:

- vaststellen van de definities van de factoren van trustworthiness en ITO-risico's;
- opstellen van interviewvragen met betrekking tot de relatie tussen de factoren van trustworthiness en ITO-risico's;
- semigestructureerde interviews afnemen;
- interviews uitwerken;
- data verzamelen en voorbereiden voor analyse;
- verzamelde data analyseren;
- analyseren, beschrijven en toetsen in welke mate de factoren invloed hebben op de ITO-risico's.

4.2 Onderzoeksstrategie

4.2.1 Onderzoeksbenadering

Dit onderzoek richt zich op het vaststellen of er al dan niet een relatie bestaat tussen risico's en vertrouwen binnen IT-outsourcing. Dit wordt gebaseerd op het reeds bestaande Model of Trust van Mayer (1995).

De factoren van het "Model of trust" van Mayer (1995) worden door de onderzoeker getracht in relatie te brengen met ITO-risico's, waarbij tevens wordt onderzocht of de perceptie van het ITO-risico kan worden beïnvloed door deze factoren. Dit deel van het onderzoek richt zich op de verdere ontwikkeling van dit model. Aangezien er binnen dit onderzoek gezocht wordt naar relaties en beïnvloeding van de perceptie van het ITO risico, wordt er niet geredeneerd vanuit een hypothese, maar vanuit waarnemingen, hetgeen betekent dat dit onderzoek de inductieve methode volgt.

Met de inductieve methode wordt een manier van redeneren bedoeld, die dient als bewijstechniek. Bij inductief redeneren komt men op grond van een aantal specifieke waarnemingen tot een algemene regel, generalisatie geheten.

De inductieve methode legt de nadruk op:

- het begrijpen van betekenis die mensen aan gebeurtenissen toekennen;
- een goed begrip van de context van het onderzoek;
- het verzamelen van kwalitatieve data;
- een flexibele structuur van het onderzoek;
- besef dat de onderzoeker onderdeel vormt van het onderzoeksproces;
- geringer belang om te generaliseren (Saunders M., 2015).

Onderzoek waarin de inductieve methode wordt gebruikt houdt zich meer bezig met de context waarbinnen de gebeurtenissen zelf plaatsvinden. Hierdoor kan een kleine steekproef geschikter zijn dan de studie van een groot aantal (Saunders M., 2015).

De onderzoeksfilosofie richt zich op het interpretivisme, wat ook wel subjectivisme of (sociaal) constructivisme wordt genoemd. Volgens deze filosofie is het noodzakelijk voor de onderzoeker om verschillen te begrijpen tussen mensen in onze rol als sociale actoren. Zodoende wordt onderscheid gemaakt tussen objecten en mensen, waarbij wij mensen sociale actoren zijn die de wereld om zich heen interpreteren. Op basis van deze interpretaties passen we onze betekenissen over de wereld om ons heen en ons gedrag aan. Voor de onderzoeker betekent dit dat deze een empathische houding aanneemt om de betekenis, die sociale actoren vormen, te kunnen begrijpen.

4.2.2 Onderzoeksdoel

Saunders (2015) stelt dat er drie onderzoeksdoelen zijn:

- Beschrijvend onderzoek, waarbij het doel is om een nauwkeurig verslag te geven van personen, gebeurtenissen of situaties;
- Verkennend (of exploratief) onderzoek, waarbij ernaar gestreefd wordt om nieuwe inzichten in verschijnselen te verkrijgen, vragen te stellen en de verschijnselen in een nieuw licht te zetten;
- Verklarend onderzoek, dat zich richt op het bestuderen van een situatie of een probleem om het verband tussen verschillende variabelen te kunnen verklaren.

Wat dit onderzoek tracht te doen is tweeledig, een verkennend onderzoek enerzijds en een verklarend onderzoek anderzijds:

1. In het eerste deel van het onderzoek wordt nagestreefd een relatie te vinden tussen ITO-risico's en de factoren van trustworthiness. Dit deel van het onderzoek tracht nieuw inzicht te verkrijgen en is hierdoor een verkennend onderzoek;
2. In het tweede deel wordt onderzocht hoe groot de invloed is van de relatie tussen de drie factoren van trustworthiness en de ITO-risico's op de totale hoogte van de perceptie van het ITO-risico. Dit deel van het onderzoek is verklarend. Als *dit* gebeurt dan is het gevolg dat er *iets* verandert of *niets* verandert.

Saunders (2015) geeft de drie belangrijkste manieren waarop verkennend onderzoek uitgevoerd kan worden:

- een literatuuronderzoek (of uitgebreider: deskresearch);
- praten met experts op het desbetreffende gebied;
- het houden van een focusinterview.

Door middel van verklarend onderzoek kunnen verbanden tussen variabelen gelegd worden en in het bijzonder oorzaak- en gevolgverbanden. Indien men kan verklaren waarom een verandering in de ene variabele een verandering in de andere variabele tot gevolg heeft, neemt de mogelijkheid om die veranderingen te voorspellen toe (Saunders M., 2015).

4.2.3 Onderzoeksmethoden

Dit onderzoek wordt uitgevoerd volgens de surveymethode. Dit onderzoek is een inductief onderzoek. Daarmee ligt het gebruik van de surveymethode niet voor de hand, maar kan wel toegepast worden. Er is door de onderzoeker gekozen om dit onderzoek uit te voeren middels de surveyonderzoek methode, omdat onderzocht wordt of de factoren van trustworthiness van Mayer (1995) invloed hebben op de twaalf geselecteerde ITO-risico's. Hierbij zal getracht worden om de sterkte van deze invloed vast te stellen. Dit zal gebeuren door middel van interviews met experts op het desbetreffende gebied. De antwoorden zullen niet op basis van een bestaande case komen, maar vanuit de kennis en ervaring van de expert. Dit onderzoek geeft antwoord op de 'wat' en 'hoeveel' vragen, daarmee past de survey strategie bij dit onderzoek. Deze motivatie voor het gebruik van deze methode is opgenomen in appendix 3. In appendix 3 wordt tevens beargumenteerd waarom andere onderzoeksstrategieën niet gebruikt worden.

Surveyonderzoek als methode wordt gewoonlijk geassocieerd met de deductieve methode. Het is een onderzoeksstrategie waarbij er op gestructureerde wijze gegevens van een vrij grote populatie worden verzameld. Bij een surveyonderzoek wordt vaak een enquête gebruikt voor het verzamelen van gegevens met behulp van vragenlijsten, maar een surveyonderzoek omvat ook andere methoden, zoals gestructureerde interviews (Saunders M., 2015).

4.2.4 Tijdshorizon

Dit onderzoek zal een dwarsdoorsnedeonderzoek worden, hetgeen betekent dat er een bepaald verschijnsel over een bepaalde korte periode wordt bestudeerd. Om een beter inzicht te verkrijgen in hoe trust zich ontwikkelt en of er daadwerkelijk bewust gestuurd kan worden op factoren van trustworthiness, zou een longitudinaal onderzoek beter passen. Het effect is namelijk pas in de tijd goed te meten. Echter, omwille van de beperkte omvang en tijd van dit onderzoek wordt gekozen voor een dwarsdoorsnedeonderzoek. Dit houdt in dat het effect op de lange termijn niet onderzocht wordt. Het onderzoek zal een bepaald punt in de tijd omvatten om de relatie tussen factoren van trustworthiness en de ITO-risico's te onderzoeken. Hierop volgend wordt onderzocht hoe groot de invloed is van de factoren van trustworthiness op de perceptie van deze risico's. Hoe hier dan bewust op gestuurd kan worden zal omwille van de tijd niet meegenomen worden in dit onderzoek.

4.2.5 Methode van gegevensverzameling

De doelstelling van dit onderzoek is inductief van aard. Bij de inductieve vorm past kwalitatieve gegevensverzameling (Saunders M., 2015).

Bij kwalitatief onderzoek wordt niet of nauwelijks met cijfermatige data gewerkt. Het doel van kwalitatief onderzoek is om iets te verkennen, te snappen. Kwalitatief onderzoek wordt vaak op kleine schaal uitgevoerd, waarbij men iets probeert te observeren en te interpreteren om vervolgens te koppelen aan de theorie. Bij kwalitatief onderzoek geeft Saunders twee vormen van gegevensverzameling: participerende waarneming en gestructureerde waarneming. Participerende waarnemingen zijn waarnemingen waarbij de onderzoeker zelf deelneemt aan het onderzoek middels participerende observatie. De gestructureerde waarnemingen binnen een kwalitatief onderzoek worden middels interviews verkregen (Saunders M., 2015).

Dit onderzoek is tevens verkennend van aard. Volgens Saunders wordt bij verkennend onderzoek gebruik gemaakt van of niet-gestructureerde interviews of semigestructureerde interviews (Saunders M., 2015). De gegevensverzameling voor dit onderzoek zal middels semigestructureerde interviewtechniek plaatsvinden, omdat de score voor de relatie tussen de factoren van trustworthiness en de ITO-risico's op een eenduidige manier verkregen en vastgelegd moet worden voor de analyse. Bij de analyse is het van belang dat de antwoorden van de respondenten op een ondubbelzinnige wijze met elkaar vergeleken worden.

De toegepaste methode van data verzamelen zal voor dit onderzoek een kwalitatief onderzoek met monomethode worden. Bij de monomethode wordt er één manier van data verzamelen gebruikt en ook één manier van analyse. Binnen dit onderzoek wordt één enkele kwalitatieve methode gebruikt voor dataverzameling en zal de data ook op één manier geanalyseerd worden, namelijk de data zullen via interviews worden verzameld en worden geanalyseerd met niet-numerieke kwalitatieve procedures.

4.2.6 Primaire gegevensverzameling

Middels semigestructureerde waarnemingen, in de vorm van semigestructureerde interviews, zal worden getracht om inzicht te krijgen in de relatie tussen factoren van trustworthiness en ITO-risico's, en hoe deze per relatie in verhouding staan tot de perceptie van het totale vertrouwen. Voor dit onderzoek wordt gekozen voor één-op-één interviews. De beweegreden hiervoor is praktisch van aard. Het is niet mogelijk om de afzonderlijke deelnemers in een groepsvorm te interviewen, want wanneer meerdere personen antwoorden geven op een vraag ontstaat hierdoor te veel ruis. De interviews zullen worden gehouden in persoon en er wordt geen gebruik gemaakt van telefonische interviews of interviews via internet.

Tijdens de interviews worden per respondent de volgende gegevens verzameld:

1. algemene informatie over de respondent en de rol van respondent in de relatie tot de ICT-leverancier;
2. informatie over de begrippen en het geven van voorbeelden door de respondent, om te toetsen of de uitleg van de begrippen helder is;
3. de toekenning door de respondent of er een relatie bestaat waarbij de factoren van trustworthiness invloed hebben op de ITO-risico's aan de hand van een Likertschaal;
4. een toelichting op de Likertscore die gegeven is bij punt drie;
5. de invloed van de relatie tussen de factor van trustworthiness en het ITO-risico op het geheel aan vertrouwen middels een rapportcijfer;
6. een toelichting op de invloed van de relatie die gegeven is bij punt vijf.

De vraag die per relatie van factor van trustworthiness en ITO-risico gesteld zal worden aan de respondenten is:

"In hoeverre bent u het eens met de stelling dat [de factor] van toepassing is op [het ITO-risico]?"

Indien van de 36 mogelijke relaties antwoorden zijn gegeven door de respondent, zal er gevraagd worden hoe groot de invloed is van deze relatie op het totaal aan vertrouwen.

4.2.7 Onderzoekspopulatie

De onderzoekspopulatie bestaat uit organisaties die hun ICT hebben geoutsourcet. Voor dit onderzoek zijn er drie organisaties uitgekozen die allen behoren tot de rijksoverheid. Tevens zijn de IT-leveranciers ook onderdeel van de rijksoverheid. Dat deze organisaties allen tot de rijksoverheid

behoren is berust op het feit dat de onderzoeker zelf werkzaam is voor de rijksoverheid en hier de contacten heeft. Er is hier geen sprake van een inhoudelijke keuze.

De drie organisaties en hun IT-leverancier zijn:

- Organisatie A outsourcet bij IT-leverancier X;
- Organisatie B outsourcet bij IT-leverancier X;
- Organisatie C outsourcet bij IT-leverancier Y;

De organisaties van zowel de klant als de IT-leverancier zijn in bovenstaande overzicht anoniem opgenomen. Dit zal geen effect hebben voor de resultaten van dit onderzoek.

Omwille van de beschikbare tijd van dit onderzoek wordt het aantal respondenten beperkt tot drie. Daarbij wordt opgemerkt dat een beperkt aantal respondenten niet geheel past bij de gekozen onderzoeksmethode, aangezien de surveymethode doorgaans wordt gebruikt voor het verzamelen van gegevens van een grote populatie.

4.2.8 Toegang tot respondenten, data en onderzoeksethiek

De onderzoeker werkt in een organisatie waarbij de IT geoutsourcet is. In deze hoedanigheid heeft de onderzoeker de functie van accountmanager, wat inhoudt dat zij de contactpersoon is tussen de organisatie en de IT-leverancier. Vanuit deze functie zal de onderzoeker de bestaande contacten als eerste benaderen om deel te nemen aan het empirisch onderzoek. Verder wordt getracht om via deze bestaande contacten aan andere respondenten voor dit onderzoek te komen.

Het doel van deelname aan het onderzoek moet vooraf duidelijk gemaakt worden aan de respondenten en daarbij moeten mogelijke voordelen voor de deelnemers helder gemaakt worden. Aan de respondenten zal tijdens het interview toestemming gevraagd worden om de gegevens te gebruiken voor het onderzoek. De uitwerkingen van elke respondent worden met een respondentnummer genoteerd. De namen van de respondenten en de relatie tussen respondent en het respondentnummer worden niet opgenomen in de verslaglegging. Daarmee is de anonimiteit van de individuele respondenten gewaarborgd.

4.3 Aanpak en verzameling van gegevens

4.3.1 Vastlegging gegevens

De interviews worden vastgelegd middels een audio opname, waarvan de relevante delen na het interview getranscribeerd worden. De relevante delen zijn in dit geval vooral de delen waarbij de respondent een antwoord geeft op de vraag of de door de onderzoeker gezochte relatie bestaat. Tevens zal er een toelichting gevraagd worden. De inleiding, toelichting van het onderzoek en het bespreken van de begrippen worden niet getranscribeerd. Op dit punt wordt volstaan met de mededeling in de transcriptie: "de onderzoeker introduceert het onderzoek" en de "onderzoeker en respondent nemen de begrippen samen door".

Tijdens het interview wordt gebruik gemaakt van een vooraf opgestelde Excel gegevensverzameling spreadsheet, waarin de antwoorden op de vragen direct worden vastgelegd. Deze vragenlijst is opgenomen in appendix 4.

4.3.2 Werkwijze interviews

Er worden semigestructureerde interviews afgenomen waarbij de antwoorden worden genoteerd in een vooraf gestructureerd antwoordvel, die is opgesteld in Excel. De vragen zijn vooraf opgesteld, waarbij de antwoorden gestructureerd worden genoteerd. De interviews worden op deze wijze afgenomen, omdat middels deze werkwijze per gestructureerde vraag en notering ruimte is voor

toelichting van de respondent. De onderzoeker kan hiermee toetsen of de respondent de vraag en het antwoord juist heeft geïnterpreteerd. De toelichting is tevens van belang bij de analyse om te beoordelen of alle respondenten eenduidige antwoorden geven.

Deel één van het onderzoek, het onderzoek naar de relatie volgens de respondent, wordt uitgewerkt in een antwoordvel dat algemene gegevens van de respondent bevat (bijvoorbeeld: functie, werkzaamheden, etc.). De gegevens met betrekking tot de gezochte relatie worden in een tabel opgenomen. In de eerste kolom staan de ITO-risico's. Op de eerste rij worden de factoren van trustworthiness, te weten ability, benevolence en integrity, benoemd. In de ontstane vakjes worden de Likertwaarden genoteerd. Iedere score krijgt een toelichting van de respondent, zodat de score tijdens de analyse in de goede context geplaatst kan worden. Dit antwoordvel is in appendix 4 opgenomen.

In deel twee wordt onderzocht welke invloed de bestaande relatie heeft, zoals benoemd in deel één, op de totale hoogte van de perceptie van het ITO-risico. Hierbij worden tijdens de semigestructureerde interviews antwoorden genoteerd in hetzelfde vooraf gestructureerde antwoordvel. De respondent wordt gevraagd, indien het ITO-risico in meer of mindere mate een relatie heeft met de factoren van trustworthiness, in welke mate er sprake is van invloed op het geheel van de perceptie van vertrouwen. Hier kan een cijfer gegeven worden van nul tot tien, waarbij nul helemaal geen invloed is en tien heel veel invloed.

Tijdens de interviews wordt de volgende werkwijze gehanteerd:

1. toestemming vragen om het interview op te nemen en om de resultaten te gebruiken voor dit onderzoek;
2. een introductie van het onderzoek, bestaande uit de uitleg over het model en de begrippen die gebruikt worden in dit onderzoek;
3. gegevensverzameling:
 - algemene informatie van de respondent en de rol van de respondent in de relatie met de IT-leverancier;
 - het beoordelen of er een relatie bestaat tussen de ITO-risico's en de factoren van trustworthiness en toelichting erop;
 - het beoordelen van de relatie op het geheel van vertrouwen en de toelichting erop.

Van deze werkwijze is door de onderzoeker een draaiboek gemaakt. Deze is in appendix 5 opgenomen.

Interviewerbias kan een rol spelen doordat het interview niet gesloten is, maar semi-gestructureerd. Er vindt interactie plaats tussen onderzoeker en respondent. Om interviewerbias te voorkomen zal de onderzoeker actief proberen zich neutraal op te stellen in het gesprek.

4.3.3 Gebruikte meetwaarden

Indien er geprobeerd wordt om iemands houding of gedrag te meten, is de Likertschaal de meest populaire manier om dit te doen. Een Likertschaal meet houding en gedrag met behulp van antwoordkeuzen die variëren van het ene uiterste naar het andere, bijvoorbeeld van *'helemaal niet waarschijnlijk'* tot *'zeer waarschijnlijk'*. De Likertschaal kan in verschillende vormen voorkomen. De 5-punts Likertschaal is de meest voorkomende antwoordschaal.

Voor het eerste deel van het onderzoek is er gekozen voor een 5-punts Likertschaal, welke hieronder is weergegeven. De belangrijke reden om niet te kiezen voor de 3-punts schaal is dat psychologisch gezien, respondenten minder geneigd zijn om uitersten in te vullen, met name wanneer het gaat om meningen en/of beoordelingen. Bij een 5-punts Likertschaal kiest men logischerwijs minder vaak

voor de uitersten, maar dit kan gecorrigeerd worden door twee categorieën samen te nemen, bijvoorbeeld 'zeer tevreden' en 'tevreden'. Ten opzichte van een 7-punts Likertschaal is een 5-punts schaal voor de respondent tevens makkelijker te begrijpen. Omdat de 7-punts schaal voor de respondent erg onoverzichtelijk en verwarrend werkt, is dit dan ook een veelvoorkomend argument tegen deze schaal.

De gegevens van de Likertschaal zijn ordinale variabelen. Dit zijn variabelen die op een bepaalde dimensie (grootte, sterkte, intensiteit) geordend kunnen worden van laag naar hoog. Metingen op ordinaal niveau kennen een natuurlijke ordening. Bij de Likertschaal zijn er verschillende categorieën aan te duiden waar verschillen tussen zitten. Hierbij is de volgorde duidelijk, maar zijn de verschillen tussen de waarden moeilijk interpreteerbaar. De 'afstand' tussen twee opeenvolgende antwoordcategorieën zoals 'neutraal' en 'eens' is niet noodzakelijkerwijs gelijk aan de 'afstand' tussen twee andere opeenvolgende antwoordcategorieën zoals 'eens' en 'geheel eens'.

De Likertschaal die bij dit onderzoek wordt gebruikt is in Tabel 2 weergegeven.

Tabel 2: *Likertschaal ten behoeve van het empirisch onderzoek*

Likertschaal	
1	geheel oneens
2	oneens
3	neutraal
4	eens
5	geheel eens

Voor het tweede deel van het onderzoek wordt een rapportcijfer gebruikt van 0 tot en met 10, waarbij 0 geen invloed is en 10 heel erg veel invloed.

In Nederland is het gebruikelijk dat op scholen en universiteiten het werk van leerlingen en studenten wordt beoordeeld door middel van een rapportcijfer van 1 tot en met 10. Men tracht hiermee een zo objectief mogelijk beoordelingssysteem te verkrijgen.

Deze rapportcijfers hebben in Nederland de volgende betekenis, zie Tabel 3.

Tabel 3: *Rapportcijfers in Nederland en de betekenis*

Cijfer	Omschrijving
10	uitstekend
9	zeer goed
8	goed
7	ruim voldoende
6	voldoende
5	twijfelachtig / zwak
4	onvoldoende
3	ruim onvoldoende
2	slecht
1	zeer slecht

Dit houdt in dat bijvoorbeeld een prestatie die als 'goed' wordt beoordeeld het cijfer 8 krijgt en een die als 'onvoldoende' beschouwd wordt het cijfer 4. Deze manier van beoordelen is in Nederland algemeen geaccepteerd en iedereen is hiermee bekend. Een kanttekening hierbij is dat op scholen de trend is om steeds minder met cijfers te werken. Een volgende generatie zal wellicht minder bekend zijn met bovenstaande cijfers en betekenissen.

Aangezien de interviews plaats vinden in Nederland met Nederlandse respondenten is gekozen voor deze methode.

4.3.4 Gebruikte software

De uitwerking en notering van de interviews gebeurt in Microsoft® Excel® voor Mac 2011, versie 14.7.1.

Er wordt gebruik gemaakt van een spreadsheet om de verzamelde gegevens in te noteren, omdat er gemakkelijk een vergelijking gemaakt kan worden tussen de gegevens. Daarnaast kan er met de gegevens gerekend worden. De keuze voor Microsoft Excel komt mede voort uit het feit dat de onderzoeker kennis heeft van dit product.

4.4 Verwerking en analyse van de gegevens

4.4.1 Verwerking

Volgens Saunders is er een aantal stappen te nemen om tot analyse van de gegevens te komen, te weten:

- datareductie;
- data weergeven (visuele weergave);
- conclusies trekken en weergeven (Saunders M., 2015).

Allereerst moet datareductie plaatsvinden door deze samen te vatten of te vereenvoudigen. Na het comprimeren kan deze data geanalyseerd worden. Dit is in het onderzoek al deels tijdens de interviews gedaan door deze semigestructureerd af te nemen en ook als zodanig te noteren.

Hierna zal in het kader van het onderzoek getracht worden om een verklaring op te bouwen. De procedure van een verklaring opbouwen verloopt, volgens Yin (2003) aangehaald door Saunders (2015), via een aantal fasen:

1. een stelling op theoretische grondslag ontwerpen, die vervolgens getoetst wordt;
2. beginnen met het verzamelen van data, om de resultaten hiervan te vergelijken met de theoretische veronderstelling;
3. indien nodig het aanpassen van de theoretische veronderstelling;
4. proces zo nodig herhalen totdat een bevredigende verklaring is gevonden (Saunders M., 2015).

4.4.2 Analyse en visualisatie

Visualisatie van de uitkomsten van de interviews, de Likertschaal gegevens, zal resulteren in een tabel waarin alle antwoorden van de respondenten zullen staan weergegeven.

De analyse vindt vervolgens plaats via analytische inductie, hetgeen wordt gedefinieerd als intensief onderzoek naar een aantal strategisch gekozen cases om zo de oorzaken van een specifiek verschijnsel empirisch vast te stellen. Middels een open manier van kijken naar de data wordt er getracht om opmerkelijke aspecten en bevindingen te vinden die vervolgens worden geclusterd.

Er zal gekeken worden naar de belangrijkste overeenkomsten en verschillen tussen de antwoorden van de respondenten. Dit zal geanalyseerd worden en er zal onderzocht worden waarom deze verschillen en overeenkomsten zich voordoen, met als doel om inzicht te verkrijgen in de relatie tussen de factoren van trustworthiness en ITO-risico's. Dit zal gebeuren door de antwoorden, de Likertwaarden, naast elkaar te leggen om de overeenkomsten te identificeren. Indien er geen overeenkomsten gevonden worden tussen de antwoorden van de respondenten, zal de analyse

plaatsvinden op de toelichtingen op de Likertwaarden. Deze zullen in deze scriptie uitgewerkt worden.

Om te onderzoeken of er een verband bestaat tussen de Likertwaarde van de relatie en het rapportcijfer van de beïnvloeding van deze relatie op het totaal aan vertrouwen, zal een correlatiecoëfficiënt toegepast worden. Met een correlatiecoëfficiënt kun je kwantificeren hoe sterk het verband is tussen twee rangorde- of numerieke variabelen is. Deze coëfficiënt, aangegeven met de letter r , kan elke waarde tussen de -1 en de +1 aannemen (Saunders M., 2015). De correlatie tussen de Likertwaarde en het rapportcijfer zal inzichtelijk worden gemaakt via een spreidingsdiagram.

4.5 Validiteit en betrouwbaarheid

4.5.1 Betrouwbaarheid

De betrouwbaarheid van het onderzoek is belangrijk, omdat er gewaarborgd dient te worden dat de verrichtingen bij herhaling dezelfde uitkomsten zullen hebben. Om te toetsen of de betrouwbaarheid van een onderzoek hoog is moet volgens Saunders bevestigend geantwoord worden op drie vragen, te weten:

1. Leveren de metingen bij andere gelegenheden dezelfde resultaten?;
2. Doen andere waarnemers gelijksoortige waarnemingen?;
3. Is de manier waarop de ruwe data zijn geïnterpreteerd transparant (Saunders M., 2015)?

De betrouwbaarheid van dit onderzoek wordt geborgd door:

- Het gebruiken maken van een gestandaardiseerde vragenlijst met daarin controlevragen. Het doel hiervan is controleren of de achtergrond van respondent in lijn is met het onderzoek;
- Audio-opname maken van de interviews, zodat het getranscribeerd kan worden. Hierdoor is het altijd mogelijk om de interviews terug te luisteren en na te lezen;
- Het toevoegen van de in dit onderzoek gebruikte tools, interviews, vragenlijsten en formulieren in de appendices van dit document. Hierdoor is het mogelijk om dit onderzoek indien gewenst te herhalen c.q. de resultaten te controleren en analyseren.

4.5.2 Validiteit

Om de interne validiteit, ofwel meten wat beoogd wordt te meten, van dit onderzoek te borgen, is het van belang dat de input helder en eenduidig is. Dit is te realiseren door helder te documenteren wat bedoeld wordt met de begrippen (zie appendix 5). Dit zorgt ervoor dat minimale begripsverwarring kan ontstaan. De begrippen moeten uitvoerig met de respondent doorgenomen worden, zodat de onderzoeker en de respondent op dezelfde lijn zitten. Daarnaast moet het, bij het bepalen van de meetwaarden van de relaties en de beïnvloeding ervan, ook voor de respondent helder zijn wat de meetwaarden zijn. Deze meetwaarden mogen niet multi-interpretabel zijn.

Bij de inhoudsvaliditeit wordt gekeken in hoeverre de semigestructureerde vragenlijst de onderzoeksvragen voldoende dekt. Dit wordt geprobeerd te ondervangen door het onderzoeksdoel en onderzoeksvragen voorgaand aan het interview uit te leggen aan de respondent. Tevens is het van belang dat de processtappen van het onderzoek goed gedocumenteerd worden en dat de gebruikte materialen toegevoegd worden aan het verslag. Hiermee kunnen de processtappen gevolgd worden en kan aannemelijk worden gemaakt dat middels de genomen processtappen er een antwoord is gevonden op de onderzoeksvragen.

4.5.3 Generaliseerbaarheid

De generaliseerbaarheid van het onderzoek is belangrijk, omdat de resultaten van het onderzoek toepasbaar moeten zijn op andere onderzoekssituaties.

Het onderzoek heeft een kleine populatie wat van invloed is op de generaliseerbaarheid. In het algemeen kan gesteld worden dat hoe kleiner de populatie is, hoe kleiner de generaliseerbaarheid. Het onderzoek wordt toegepast op meerdere relaties van verschillende respondenten om binnen deze beperking tot een zo hoog mogelijke generaliseerbaarheid te komen.

4.6 Vooruitblik op resultaat

De verwachting is dat de factoren van trustworthiness een relatie hebben met de geselecteerde ITO-risico's en dat deze invloed hebben op de perceptie van het vertrouwen. Indien hier sprake van is, is de verwachting dat de factoren van trustworthiness elk op hun eigen manier correleren met de ITO-risico's. Deze verschillende correlatie van factoren zal ervoor zorgen dat op een bepaalde manier invloed wordt uitgeoefend op de totale hoogte van de perceptie van vertrouwen.

Dit onderzoek zal de volgende resultaten opleveren:

- de relaties tussen de ITO-risico's en de factoren van trustworthiness;
- de invloed die de factoren hebben op de verschillende ITO-risico's;
- een ordening in ITO-risico lijst. Welke ITO-risico's hebben een relatie met de factoren van trustworthiness en in welke mate? Indien de factoren een relatie hebben met de ITO-risico's, maar de factoren zijn niet te beïnvloeden, dan kan hierop niet bewust gestuurd worden. Dan is deze relatie van minder belang;
- analyse van de relaties. Zijn deze verschillend per ITO-risico en per factor?;
- conclusie van de analyse;
- aanbevelingen voor nader onderzoek naar aanleiding van de casestudy. Waar zijn de respondenten het met elkaar eens en waar zijn ze het niet met elkaar eens? Indien de respondenten het met elkaar eens zijn, dan kan dit als generiek geconcludeerd worden. Daarnaast kunnen verschillen in de beantwoording van de respondenten interessant zijn, omdat dit een aanleiding kan zijn voor nader onderzoek. Wat zijn de oorzaken hiervan? Kan het op grote schaal onderzocht worden en waar moet dan rekening mee gehouden worden?

5 Uitvoering

In de uitvoeringsfase verschilt de lijst met ITO-risico's van de lijst zoals deze is opgesteld in het literatuuronderzoek. Er is nog steeds sprake van twaalf ITO-risico's, echter is het risico *goal incongruence* uit het risico genaamd *single/double moral hazard* gehaald. Tevens is *shirking* ondergebracht in het risico *opportunistic behaviour*, omdat uit de literatuur blijkt dat dit onderdeel is van dit risico. Dit inzicht is verkregen tijdens het voorbereiden van de interviews en het uitwerken van de begrippen.

De gegevensverzameling heeft plaatsgevonden in maart en april van het jaar 2017. Er zijn in totaal drie respondenten geïnterviewd. De geselecteerde respondenten zijn personen die bepalend zijn in de relatie met de IT-leverancier. Er is uitgezocht of de relatie tussen de respondent en de IT-leverancier alle ITO-risico's dekt. Met andere woorden, kunnen deze geïnterviewde personen een duidelijk beeld schetsen van een eventuele relatie tussen ITO-risico's en de factoren van trustworthiness en kunnen zij daarbij een prioritering aangeven? De interviews vonden plaats bij de organisatie van de respondent in een rustige omgeving.

De onderzoeker heeft in haar rol als accountmanager van een outsourcende organisatie ook een Likertwaarde van de relaties en invloed van deze relaties ingevuld. De onderzoeker is bewust van het feit dat hier onderzoekersbias kan plaatsvinden, aangezien de verwachtingen van de onderzoeker

haar waarneming kleuren. De onderzoeker heeft toch gekozen voor deze werkwijze, mede om te toetsen of twee personen die dezelfde relatie hebben (zelfde organisatie en zelfde IT-leverancier) komen tot eenduidige antwoorden. De antwoorden van respondent 4 zijn de antwoorden van de onderzoeker zelf. De interpretatie kan ook zonder deze antwoorden gedaan worden indien dit gewenst is.

Samen met de antwoorden van de onderzoeker komt het aantal respondenten op vier (n=4). In Tabel 3 is te zien dat er binnen het onderzoek drie verschillende organisaties (A, B en C) zijn onderzocht die de IT hebben uitbesteed aan een IT-leverancier en dat er twee verschillende IT-leveranciers zijn (X en Y). Daarbij geldt dat er drie verschillende relaties zijn tussen klant en leverancier, waarbij twee personen (waaronder de onderzoeker) één en dezelfde relatie hebben. Hierbij moet vermeld worden dat alle organisaties, zowel de klanten als de IT-leveranciers, tot de rijksoverheid behoren. De organisaties van zowel de klant als de IT-leverancier zijn in Tabel 4 anoniem opgenomen.

Tabel 4: *Overzicht respondenten*

Respondent	Organisatie	IT-leverancier	Functie	Werkzaamheden	Rol / Relatie tot IT-leverancier
R1	A	X	Informatiemanager	Contractmanagement, aansturing regiefunctie, vervanging accountmanagement, gedelegeerd opdrachtgever.	Aanspreekpunt voor tactische samenwerking
R2	B	X	Informatiemanager	Afspraken met technisch beheerders van IT -leveranciers /letten op serviceniveau van de afdeling	Aanspreekpunt voor afspraken over het jaar heen.
R3	C	Y	Team coördinator	Klant- advies- en leveranciersmanagem nt	Leveranciersmanager
R4	A	X	Accountmanager	Regie op IT-leverancier	Accountmanager

Aan de respondenten is vooraf aan het interview een document verstrekt met de begrippen zoals deze in het onderzoek worden gehanteerd. Aan de respondenten is gevraagd deze door te nemen als voorbereiding op het interview. Tijdens het interview hebben onderzoeker en respondent deze begrippen samen besproken en heeft de onderzoeker daar waar nodig nog een toelichting gegeven. Deze begrippen zijn in appendix 5 opgenomen.

Tijdens het interview heeft de onderzoeker de benodigde gegevens verzameld en zijn er audio-opnames van de interviews gemaakt. De gegevensverzameling bevat per respondent het uitwerkformulier van het interview, welke in appendix 7 is opgenomen. De audio-opnames zijn getranscribeerd per respondent, deze transcripties zijn in appendix 8 is opgenomen.

6 Resultaten

6.1 Verzamelde gegevens

De resultaten van de gegevensverzameling van de vier respondenten zijn in Tabel 5 weergegeven. De antwoorden van de respondenten, met betrekking tot de relatie tussen de factor van trustworthiness en het ITO-risico, hebben zij gegeven op basis van de Likertschaal en zijn in de tweede tot en met de vijfde kolom weergegeven. Hierbij geldt dat R1 is respondent één, R2 is respondent twee, R3 is respondent drie en R4 is respondent vier. De Likertschaal ziet er als volgt uit; 1=geheel oneens, 2=oneens, 3=neutraal, 4=eens en 5=geheel eens. Aan de rechterkant van Tabel 5 zijn de rapportcijfers weergegeven die elke respondent heeft gekwalificeerd ten opzichte van de invloed die de relatie heeft op het totaal aan vertrouwen. Indien er geen relatie werd gezien door de respondent en een Likertwaarde van 1 werd toegewezen, dan heeft deze relatie ook geen invloed op het geheel aan vertrouwen en is er de waarde 0 ingevuld.

Tabel 5: *Totale gegevensverzameling per respondent*

Relatie tussen ITO-risico en factor of trustworthiness					Invloed relatie				
	R1	R2	R3	R4	R1	R2	R3	R4	
Is de factor Ability van toepassing op Backlash from internal IT staff ?	4	4	1	1	7	8	0	0	
Is de factor Benevolence van toepassing op Backlash from internal IT staff ?	4	4	4	4	9	7	7	8	
Is de factor Integrity van toepassing op Backlash from internal IT staff ?	4	4	5	4	9	7	9	8	
Is de factor Ability van toepassing op Contractual risk ?	5	4	4	5	10	8	8	9	
Is de factor Benevolence van toepassing op Contractual risk ?	5	4	5	4	10	6	8	7	
Is de factor Integrity van toepassing op Contractual risk ?	5	4	4	5	10	7	8	9	
Is de factor Ability van toepassing op Coordination between client and supplier ?	4	2	5	5	6	3	10	9	
Is de factor Benevolence van toepassing op Coordination between client and supplier ?	5	4	2	5	8	9	5	9	
Is de factor Integrity van toepassing op Coordination between client and supplier ?	5	4	5	4	9	8	10	7	
Is de factor Ability van toepassing op Cultural differences between client and supplier ?	4	1	1	5	6	0	0	8	

Resultaten: Verzamelde gegevens

Is de factor Benevolence van toepassing op Cultural differences between client and supplier ?	4	5	5	5
Is de factor Integrity van toepassing op Cultural differences between client and supplier ?	4	4	5	4
Is de factor Ability van toepassing op Difficulty in managing remote teams ?	5	4	5	5
Is de factor Benevolence van toepassing op Difficulty in managing remote teams ?	4	4	4	3
Is de factor Integrity van toepassing op Difficulty in managing remote teams ?	1	4	4	3
Is de factor Ability van toepassing op Lack of trust ?	5	5	4	5
Is de factor Benevolence van toepassing op Lack of trust ?	5	5	3	5
Is de factor Integrity van toepassing op Lack of trust ?	5	4	5	5
Is de factor Ability van toepassing op Loss of control over data ?	5	4	5	5
Is de factor Benevolence van toepassing op Loss of control over data ?	5	4	1	4
Is de factor Integrity van toepassing op Loss of control over data ?	5	5	5	4
Is de factor Ability van toepassing op Opportunistic behaviour ?	4	4	1	1
Is de factor Benevolence van toepassing op Opportunistic behaviour ?	5	5	4	4
Is de factor Integrity van toepassing op Opportunistic behaviour ?	5	5	5	5
Is de factor Ability van toepassing op Security / privacy breach ?	5	4	5	5
Is de factor Benevolence van toepassing op Security / privacy breach ?	5	4	3	3
Is de factor Integrity van toepassing op Security / privacy breach ?	5	4	4	4
Is de factor Ability van toepassing op Single / Double moral hazard ?	1	3	1	1
Is de factor Benevolence van toepassing op Single / Double moral hazard ?	4	4	5	5
Is de factor Integrity van toepassing op Single / Double moral hazard ?	5	4	4	4
Is de factor Ability van toepassing op Goal Incongruence ?	1	2	4	4
Is de factor Benevolence van toepassing op Goal Incongruence ?	4	5	4	5
Is de factor Integrity van toepassing op Goal Incongruence ?	2	5	4	4
Is de factor Ability van toepassing op Supplier employees have poor communication skills ?	4	4	5	5
Is de factor Benevolence van toepassing op Supplier employees have poor communication skills ?	4	4	4	4
Is de factor Integrity van toepassing op Supplier employees have poor communication skills ?	1	4	1	1

8	9	9	9
9	7	10	6
8	7	10	9
7	7	8	6
0	7	7	4
10	8	9	10
10	7	7	10
10	7	10	10
8	7	10	10
8	7	0	7
10	8	10	8
7	7	0	0
9	9	8	8
9	9	9	10
10	7	10	10
8	7	6	5
10	7	8	8
0	6	0	0
7	7	10	8
10	8	8	7
0	4	8	6
8	8	8	9
4	7	7	8
7	8	10	10
7	8	8	9
0	8	0	0

6.2 Verwerking van de gegevens

Aan de hand van de verzamelde gegevens is de onderzoeker begonnen met de verwerking hiervan. Om inzicht te krijgen in hoe de respondenten in relatie met elkaar geantwoord hebben, heeft de onderzoeker een overzicht gemaakt met daarin de antwoorden van de vier respondenten op een bepaalde stelling, zie Tabel 6. Aan de hand van deze Tabellen 5 en 6 kan de onderzoeker de gegevens analyseren en vergelijken met elkaar. Vanuit de analyse van deze gegevens kan er een antwoord op de onderzoeksvragen gevonden worden. Deze tabellen zijn geanalyseerd door de onderzoeker en worden in paragraaf 6.3 besproken.

Tabel 6: *Aantal Likertwaarden gegeven per relatie (factor van trustworthiness in relatie tot het ITO-risico)*

Factoren van trustworthiness	Ability					Benevolence					Integrity				
	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
ITO-Risico's															
Backlash from internal IT staff	2			2					4					3	1
Contractual risk				2	2				2	2				2	2
Coordination between client and supplier		1		1	2		1		1	2				2	2
Cultural differences between client and supplier	2			1	1				1	3				3	1
Difficulty in managing remote teams				1	3			1	3		1		1	2	
Lack of trust				1	3			1		3				1	3
Loss of control over data				1	3	1			2	1				1	3
Opportunistic behaviour	2			2					2	2					4
Security / privacy breach				1	3			2	1	1				3	1
Single / Double moral hazard	3		1						2	2				3	1
Goal Incongruence	1	1		2					2	2		1		2	1
Supplier employees have poor communication skills				2	2					4	3			1	

6.3 Analyse van de gegevens

6.3.1 Analyse van de gegevens voor onderzoeksvraag één

Voor de analyse en beoordeling van de resultaten van de verzamelde gegevens zijn de overeenkomsten en verschillen interessant, omdat inzicht verkregen kan worden in de mogelijke relatie tussen de factoren van trustworthiness en de ITO-risico's. Hiermee kan een antwoord gevonden worden op de eerste onderzoeksvraag; **in hoeverre bestaat er een invloed van één of meerdere factoren van trustworthiness op de perceptie van IT-outsourcing risico's?**

Om deze verschillen en overeenkomsten te identificeren heeft de onderzoeker de Likertschaal waarden gehergroepeerd, zodat er drie categorieën overblijven. De reden voor deze hergroepering is te vinden in de Likertwaarden 'geheel eens', 'eens', 'oneens' en 'geheel oneens'. Tijdens de interviews kwam namelijk naar voren dat, indien een relatie gezien werd, er door de respondent werd gekozen voor een Likertwaarde 'eens' of 'geheel eens'. De reden voor het verschil tussen deze twee waarden kwam vooral voort uit hoe de respondenten de beïnvloeding van deze relatie zagen op het totaal aan vertrouwen; de respondenten waren in feite al bezig met het beoordelen van de beïnvloeding van de relatie. Voor de waarden 'oneens' en 'geheel oneens' gold hetzelfde. Indien de respondent niet zeker wist of er een relatie bestaat tussen de factor en het ITO-risico werd in het algemeen voor neutraal gekozen. Op basis van voorgaande heeft de onderzoeker drie categorieën gemaakt:

- **categorie één**, er is een relatie tussen de factor van trustworthiness en het ITO-risico;
- **categorie twee**, er kan een relatie zijn tussen de factor van trustworthiness en het ITO-risico, maar het kan ook niet zijn;
- **categorie drie**, er is geen relatie tussen de factor van trustworthiness en het ITO-risico.

De **eerste categorie** is dat er **een relatie** bestaat, hieronder vallen de waarden 'geheel eens' (score vijf) en 'eens' (score vier). De **tweede categorie** is '**neutraal**' (score drie). De **derde categorie** is dat er **geen relatie** bestaat, hieronder vallen de waarden 'geheel oneens' (score één) en 'oneens' (score twee) samen. Bijvoorbeeld, de respondenten hebben een relatie beoordeeld door de volgende Likertwaarden te geven; respondent één, drie en vier geven alle drie een Likertwaarde van 'geheel oneens' en respondent twee een Likertwaarde van 'oneens'. De onderzoeker is ervan uitgegaan dat er geen relatie gezien wordt, dus in categorie drie (geen relatie) valt en dat dit een overeenkomst tussen de antwoorden van de vier respondenten is.

De overeenkomsten en verschillen zijn door de onderzoeker geanalyseerd en uitgewerkt. Eerst zullen de overeenkomsten besproken worden in paragraaf 6.3.1.1 en de verschillen in paragraaf 6.3.1.2.

6.3.1.1 Overeenkomsten in de beantwoording van de respondenten

De overeenkomsten zijn onderzocht en de categorie indeling is in Tabel 7 weergegeven.

Tabel 7: Categorie indeling van de relaties

Factoren van trustworthiness ITO-Risico's	Ability	Benevolence	Integrity
Backlash from internal IT staff	-	Categorie 1	Categorie 1
Contractual risk	Categorie 1	Categorie 1	Categorie 1
Coordination between client and supplier	-	-	Categorie 1
Cultural differences between client and supplier	-	Categorie 1	Categorie 1
Difficulty in managing remote teams	Categorie 1	-	-
Lack of trust	Categorie 1	-	Categorie 1
Loss of control over data	Categorie 1	-	Categorie 1
Opportunistic behaviour	-	Categorie 1	Categorie 1
Security / privacy breach	Categorie 1	-	Categorie 1
Single / Double moral hazard	-	Categorie 1	Categorie 1
Goal Incongruence	-	Categorie 1	-
Supplier employees have poor communication skills	Categorie 1	Categorie 1	-

Zoals in Tabel 7 te zien is, zijn er in totaal 36 mogelijke relaties tussen de drie factoren van trustworthiness en de twaalf ITO-risico's. De antwoorden van de respondenten komen in 22 relaties overeen met elkaar. Hierbij valt op, dat indien er een overeenkomst gevonden wordt tussen de antwoorden van de respondenten, deze altijd valt in categorie één.

6.3.1.2 Verschillen in beantwoording van de respondenten

Indien de meningen van de respondenten verdeeld zijn over meer dan twee Likertwaarden of Likertwaarden die tegenovergesteld zijn van elkaar ('geheel oneens' en 'eens') is dit voor de onderzoeker reden geweest om deze relatie nader te onderzoeken. Van de 36 relaties zijn de antwoorden van de respondenten van veertien relaties niet in overeenstemming met elkaar, zie Tabel 8.

Tabel 8: Relatie waarbij afwijkingen bestaan in de antwoorden van de respondenten

Relatie
De factor Ability is van toepassing op Backlash from internal IT staff
De factor Ability is van toepassing op Coordination between client and supplier
De factor Benevolence is van toepassing op Coordination between client and supplier
De factor Ability is van toepassing op Cultural differences between client and supplier
De factor Benevolence is van toepassing op Difficulty in managing remote teams
De factor Integrity is van toepassing op Difficulty in managing remote teams
De factor Benevolence is van toepassing op Lack of trust
De factor Benevolence is van toepassing op Loss of control over data
De factor Ability is van toepassing op Opportunistic behaviour
De factor Benevolence is van toepassing op Security / privacy breach
De factor Ability is van toepassing op Single / Double moral hazard
De factor Ability is van toepassing op Goal incongruence
De factor Integrity is van toepassing op Goal incongruence
De factor Integrity is van toepassing op Supplier employees have poor communication skills

Van deze veertien relaties zijn er zes relaties die betrekking hebben op de factor ability, vijf relaties die betrekking hebben op benevolence en drie op integrity. Daarbij zijn drie ITO-risico's dubbel betrokken bij een relatie waarover geen overeenstemming is; dit zijn 'coordination between client and supplier', 'difficulty in managing remote teams' en 'goal incongruence'.

Hieronder wordt de analyse per relatie, zoals deze is benoemd in Tabel 8, uitgewerkt. Hierbij worden per relatie de relevante elementen uit de interviews opgesomd. Als context wordt bij elke relatie de Likertwaarde getoond per respondent. Citaten zijn geplaatst tussen aanhalingstekens en cursief afgedrukt (voorbeeld: *"citaat"*), en er wordt in de tekst naar respondenten verwezen door het respondentnummer tussen blokhaken te plaatsen. Het totale overzicht van alle relaties is in appendix 10, Tabel 11 opgenomen.

*De factor **Ability** is van toepassing op **Backlash from internal IT staff***

Percentage antwoorden m.b.t. Relatie					Likertwaarden per respondent			
geheel oneens (1)	oneens (2)	neutraal (3)	eens (4)	geheel eens (5)	R1	R2	R3	R4
50%	0%	0%	50%	0%	4	4	1	1

Tijdens de interviews bleek deze vraag lastig te beantwoorden en duurde het ook lang voordat er een antwoord kwam. Er wordt een relatie gezien, maar bij deze relatie wordt meer gekeken naar de bekwaamheid van de interne medewerkers, dan de bekwaamheid van de IT-leverancier [R1] [R2].

De respondenten die geen relatie zien, bekijken de bekwaamheid vanuit de zijde van de leverancier [R3][R4]. *"Dat vind ik vooral iets emotioneels. En ik denk dat die eerder aanslaan op zaken als integrity en welwillendheid. Ik denk dat dat meer de relatie beïnvloedt dan de ability, want daar zit een stukje onzekerheid bij en die ga je niet weghalen door de ability van de IT-leverancier."* [R3]

*De factor **Ability** is van toepassing op **Coordination between client and supplier***

Percentage antwoorden m.b.t. Relatie					Likertwaarden per respondent			
geheel oneens (1)	oneens (2)	neutraal (3)	eens (4)	geheel eens (5)	R1	R2	R3	R4
0%	25%	0%	25%	50%	4	2	5	5

De respondent die het oneens is met deze relatie, ziet het risico meer als een relationeel aspect [R2]. Een andere respondent is het hier mee eens, maar geeft toch aan dat er wel een relatie is, alleen dat de invloed van deze relatie niet groot is gezien het relationele aspect [R1]. De andere twee respondenten stellen juist dat er vaardigheden nodig zijn om een goede coördinatie te bewerkstelligen [R3][R4], *"want het gaat om vaardigheden, sociale vaardigheden onder andere en administratieve vaardigheden, die zijn daar wel van belang"* [R3].

*De factor **Benevolence** is van toepassing op **Coordination between client and supplier***

Percentage antwoorden m.b.t. Relatie					Likertwaarden per respondent			
geheel oneens (1)	oneens (2)	neutraal (3)	eens (4)	geheel eens (5)	R1	R2	R3	R4
0%	25%	0%	25%	50%	5	4	2	5

Respondenten die benevolence wel van toepassing vinden op het risico coordination between client and supplier geven aan dat er geen goede coördinatie kan plaatsvinden zonder welwillendheid.

[R1][R2][R3]. De respondent die het hier niet mee eens is stelt: “Dat je op basis van iemands welwillendheid niet gelijk het vertrouwen beschaamt” [R3].

De factor Ability is van toepassing op Cultural differences between client and supplier

Percentage antwoorden m.b.t. Relatie				
geheel oneens (1)	oneens (2)	neutraal (3)	eens (4)	geheel eens (5)
50%	0%	0%	25%	25%

Likertwaarden per respondent			
R1	R2	R3	R4
4	1	1	5

Er wordt gesteld door respondenten die een relatie zien tussen bekwaamheid en cultural differences between client and supplier dat je bekwaam moet zijn om hiermee om te gaan [R4]. Verder wordt gesteld dat bekwaamheid niet in elke cultuur hetzelfde is, maar dat dit wel meetbaar gemaakt kan worden [R1]. Door de andere respondenten wordt gesteld dat er geen relatie is, omdat dit risico meer te maken heeft met welwillendheid en integriteit.

De factor Benevolence is van toepassing op Difficulty in managing remote teams

Percentage antwoorden m.b.t. Relatie				
geheel oneens (1)	oneens (2)	neutraal (3)	eens (4)	geheel eens (5)
0%	0%	25%	75%	0%

Likertwaarden per respondent			
R1	R2	R3	R4
4	4	4	3

Bij deze relatie liggen de antwoorden zeer dicht bij elkaar. Respondent 4 is echter niet overtuigd van een relatie en heeft hierom neutraal geantwoord, hetgeen niet uitsluit dat er geen relatie zou kunnen zijn. De overige respondenten geven aan dat welwillendheid van belang is, namelijk “de wil om de problematiek op te lossen” [R1].

De factor Integrity is van toepassing op Difficulty in managing remote teams

Percentage antwoorden m.b.t. Relatie				
geheel oneens (1)	oneens (2)	neutraal (3)	eens (4)	geheel eens (5)
25%	0%	25%	50%	0%

Likertwaarden per respondent			
R1	R2	R3	R4
1	4	4	3

Integrity in relatie tot difficulty in managing remote teams wordt door twee respondenten gezien, omdat het werken op afstand integer werk vereist. Anders is dit niet te managen [R2][R3]. De andere twee respondenten zien er wellicht geen relatie [R4] of helemaal geen relatie in [R1].

De factor Benevolence is van toepassing op Lack of trust

Percentage antwoorden m.b.t. Relatie				
geheel oneens (1)	oneens (2)	neutraal (3)	eens (4)	geheel eens (5)
0%	0%	25%	0%	75%

Likertwaarden per respondent			
R1	R2	R3	R4
5	5	3	5

De respondenten zitten bijna allemaal op dezelfde lijn, echter respondent 3 heeft een neutrale waarde op de Likertschaal gegeven. Uit het interview komt naar voren dat deze respondent wel een relatie ziet, echter is deze minder sterk dan de factoren ability en integrity [R3].

De factor Benevolence is van toepassing op Loss of control over data

Percentage antwoorden m.b.t. Relatie				
geheel oneens (1)	oneens (2)	neutraal (3)	eens (4)	geheel eens (5)
25%	0%	0%	50%	25%

Likertwaarden per respondent			
R1	R2	R3	R4
5	4	1	4

Één respondent ziet geheel geen relatie tussen benevolence en loss of control over data, hij wijt dit meer aan bekwaamheid en integriteit: *“als je met de beste wil van de wereld, het is veilig of niet, iemand is integer of niet, welwillendheid heeft daar weinig invloed op”* [R3]. De andere respondenten zien benevolence meer vanuit het punt dat de IT-leverancier welwillend is om zo goed mogelijk voor de data te zorgen [R1][R2][R4].

De factor Ability is van toepassing op Opportunistic behaviour

Percentage antwoorden m.b.t. Relatie				
geheel oneens (1)	oneens (2)	neutraal (3)	eens (4)	geheel eens (5)
50%	0%	0%	50%	0%

Likertwaarden per respondent			
R1	R2	R3	R4
4	4	1	1

Respondenten stellen dat, indien men zich opportunistisch opstelt, men niet bekwaam is [R1][R2] of juist heel erg bekwaam en heel goed weet waar men mee bezig is [R1]. Respondenten drie en vier zien hier geen relatie, want, indien men dit gedrag vertoont, vaardigheid hier niets mee te maken heeft. Het risico zit in benevolence en integriteit [R3].

De factor Benevolence is van toepassing op Security / privacy breach

Percentage antwoorden m.b.t. Relatie				
geheel oneens (1)	oneens (2)	neutraal (3)	eens (4)	geheel eens (5)
0%	0%	50%	25%	25%

Likertwaarden per respondent			
R1	R2	R3	R4
5	4	3	3

Deze relatie wordt door alle respondenten gezien, echter is de mate waarin deze relatie van invloed is op het totaal aan vertrouwen verschillend. Respondent drie geeft een neutrale waarde op de Likertschaal, maar zegt later in het interview: *“Als iemand niet welwillend is, dan heeft dat invloed op zijn motivatie en dan zakt toch zijn aandachtsniveau en dan heeft dat toch effect”* [R3].

De factor Ability is van toepassing op Single / Double moral hazard

Percentage antwoorden m.b.t. Relatie				
geheel oneens (1)	oneens (2)	neutraal (3)	eens (4)	geheel eens (5)
75%	0%	25%	0%	0%

Likertwaarden per respondent			
R1	R2	R3	R4
1	3	1	1

Respondenten één, drie en vier zijn van mening dat er geen relatie bestaat, respondent twee twijfelt. In het interview zegt respondent twee hierover: *“Ik denk dat niet zozeer bekwaamheid met moraal te maken heeft”* [R2]. Op basis hiervan kan gesteld worden dat er overeenstemming is tussen de respondenten.

De factor Ability is van toepassing op Goal incongruence

Percentage antwoorden m.b.t. Relatie				
geheel oneens (1)	oneens (2)	neutraal (3)	eens (4)	geheel eens (5)
25%	25%	0%	50%	0%

Likertwaarden per respondent			
R1	R2	R3	R4
1	2	4	4

Dit is een relatie waar de ene helft van de respondenten een relatie ziet en de andere helft niet. De respondenten die het wel zien, zijn van mening dat het met de vaardigheden van de leverancier te maken heeft, omdat de leverancier de vaardigheid moet hebben om rekening te houden met de persoonlijke doelstellingen van de medewerkers van de klant. Indien de leverancier deze vaardigheid niet bezit, dan is het resultaat informatie-asymmetrie tussen klant en leverancier. Een leverancier moet in staat zijn om de persoonlijke doelstellingen van de werknemers van de klant te zien en er op te kunnen spelen [R3][R4].

De factor Integrity is van toepassing op Goal incongruence

Percentage antwoorden m.b.t. Relatie				
geheel oneens (1)	oneens (2)	neutraal (3)	eens (4)	geheel eens (5)
0%	25%	0%	50%	25%

Likertwaarden per respondent			
R1	R2	R3	R4
2	5	4	4

Drie respondenten zijn van mening dat hier een relatie bestaat, omdat, indien een leverancier niet integer is, deze er ook niet voor kan zorgen dat de persoonlijke doelstellingen van de werknemers worden behaald. Respondent één vond dit een lastige en zag geen duidelijke relatie.

De factor Integrity is van toepassing op Supplier employees have poor communication skills

Percentage antwoorden m.b.t. Relatie				
geheel oneens (1)	oneens (2)	neutraal (3)	eens (4)	geheel eens (5)
75%	0%	0%	25%	0%

Likertwaarden per respondent			
R1	R2	R3	R4
1	4	1	1

Respondenten één, drie en vier zien geen relatie tussen integrity en het risico supplier employees have poor communication skills. *“Oplichters die kunnen vaak perfect communiceren, waarom? Dat is voor hun heel erg belangrijk om hun doel te bereiken. Dat zegt niks over hun integriteit, het zegt wel iets over het feit dat ze heel gemotiveerd zijn om het te doen en dat ze ook de vaardigheid hebben.”* [R3]. Respondent twee ziet wel een relatie, omdat ze het gebrek aan communicatieve vaardigheden ook kunnen hebben verdoezeld en dan raakt dit integriteit [R2].

6.3.2 Analyse van de gegevens voor onderzoeksvraag twee

De resultaten met betrekking tot de Likertwaarden van de relaties zijn in paragraaf 6.3.1 afgerond en gaan over in de analyse van de beïnvloeding van deze relaties op het totaal aan vertrouwen. Deze zijn vastgesteld door middel van rapportcijfers van één tot tien.

Deze rapportcijfers worden geanalyseerd om antwoord te krijgen op het tweede deel van het onderzoek; **indien er invloed is op de perceptie van ITO-risico's, hoe sterk is deze invloed?**

De rapportcijfers van de beïnvloeding van de relatie op het totale vertrouwen heeft de onderzoeker nader onderzocht. Hieruit blijkt dat het rapportcijfer dat gegeven wordt, in de meeste gevallen ongeveer een verdubbeling is van de door de respondent vastgestelde Likertwaarde. Dit is een

eerste aanwijzing voor een correlatie tussen deze twee waarden. Bijvoorbeeld, op een relatie is een Likertwaarde van vier vastgesteld, voor de beïnvloeding wordt een rapportcijfer van acht gegeven. Hierbij heeft de onderzoeker geconstateerd dat in de meeste gevallen er een verdubbeling van de Likertwaarde is, of dat er een verdubbeling met een afwijking van één is. In zestien antwoorden is er een afwijking van twee op de verdubbeling van de Likertwaarde, en in een tweetal gevallen is er een verdubbeling met een afwijking van drie. Zie appendix 9 voor het overzicht, Tabel 10, van de scores en de afwijkingen.

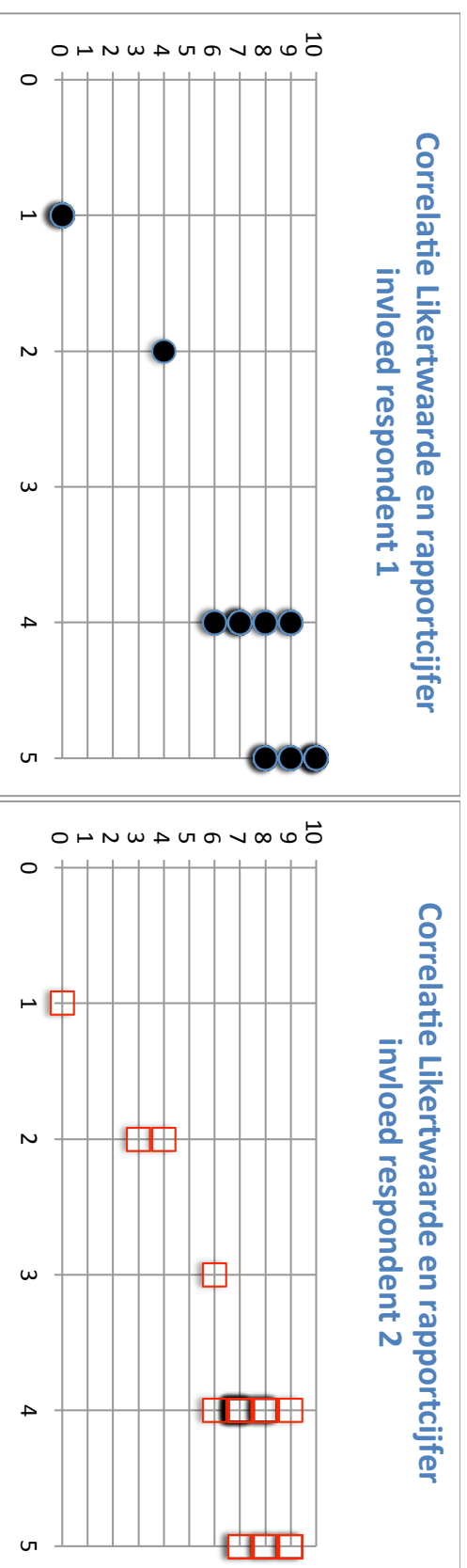
Om statistisch te onderzoeken of er daadwerkelijk een correlatie bestaat tussen de Likertwaarde van de relatie en de beïnvloeding van deze relatie op het totaal aan vertrouwen, is een correlatiecoëfficiënt toegepast. De correlatiecoëfficiënt is een getal tussen de +1 en de -1 die de sterkte van het verband aangeeft tussen twee geordende of kwantificeerbare variabelen. Een waarde gelijk aan +1 vertegenwoordigt een perfecte positieve correlatie. Een waarde gelijk aan -1 vertegenwoordigt een perfecte negatieve correlatie. Correlatiecoëfficiënten tussen +1 en -1 vertegenwoordigen zwakkere positieve en negatieve correlaties, waarbij een waarde gelijk aan 0 betekent dat de variabelen volkomen onafhankelijk zijn (Saunders M., 2015).

Aangezien beide variabelen numerieke data bevatten, is de Pearson product moment correlatiecoëfficiënt (PMCC), ook wel r genoemd, gebruikt. De formule van PMCC is Figuur 2 afgebeeld.

$$r = \frac{n \sum xy - \sum x \sum y}{\sqrt{(n \sum x^2 - (\sum x)^2)(n \sum y^2 - (\sum y)^2)}}$$

Figuur 2: Pearson product moment correlatiecoëfficiënt (r)

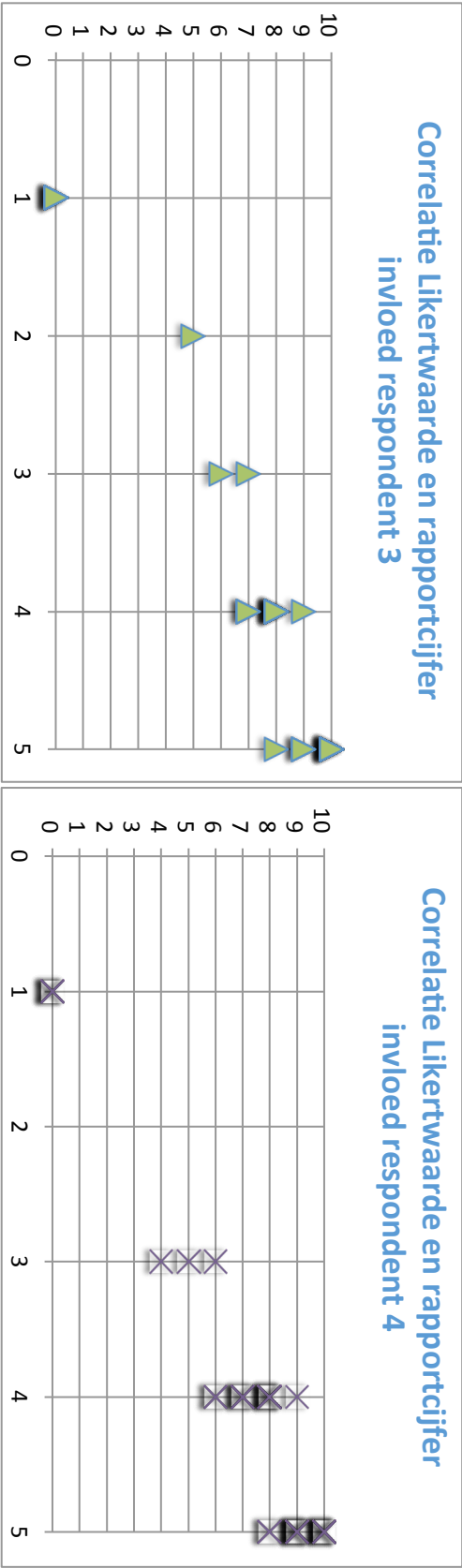
De correlatie tussen de Likertwaarde en het rapportcijfer van de invloed van de relatie, is per respondent inzichtelijk gemaakt via een spreidingsdiagram.



Figuur 3: correlatie Likertwaarden en rapportcijfers respondent 1

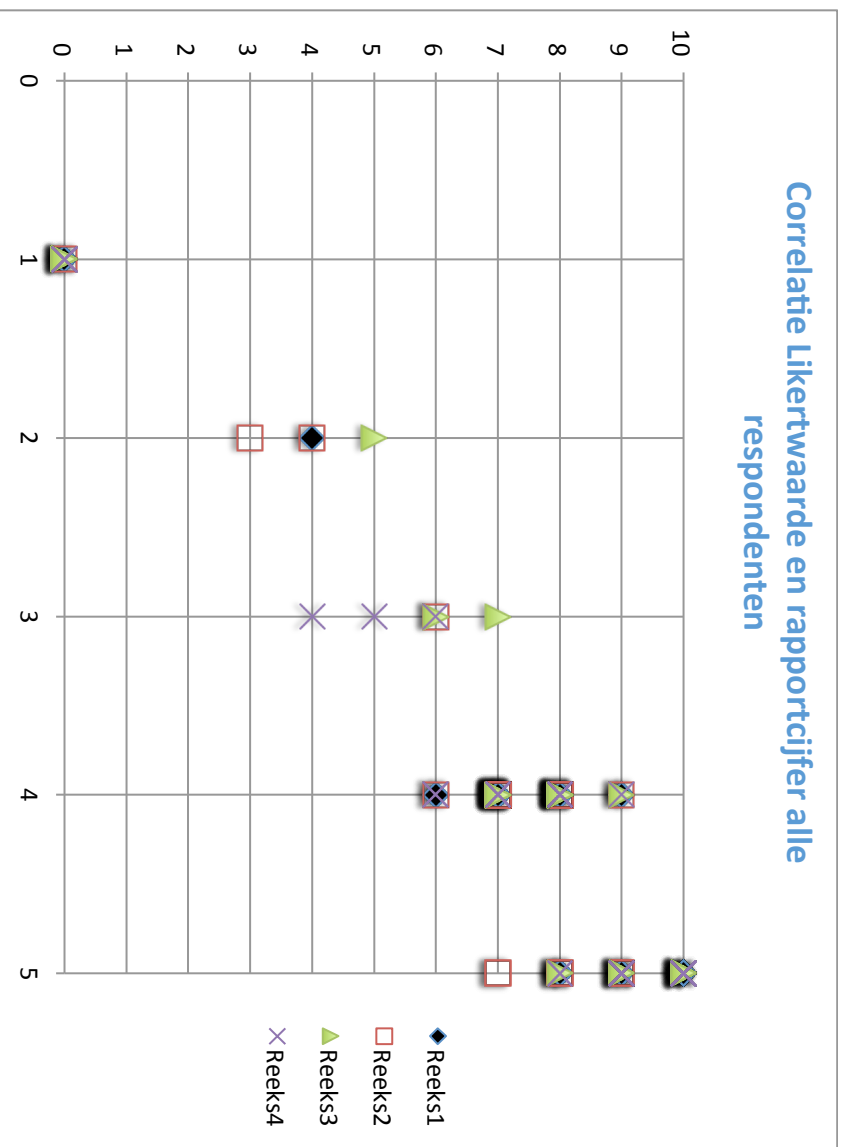
Figuur 4: correlatie Likertwaarden en rapportcijfers respondent 2

De correlatiecoëfficiënt, van de correlatie tussen de Likertwaarden en de bijbehorende rapportcijfers, van respondent 1 is 0,95085926 (zie Figuur 3). De correlatiecoëfficiënt, van de correlatie tussen de Likertwaarden en de bijbehorende rapportcijfers, van respondent 2 is 0,874303922 (zie Figuur 4).



Figuur 5: correlatie Likertwaarden en rapportcijfers respondent 3 *Figuur 6:* correlatie Likertwaarden en rapportcijfers respondent 4

De correlatiecoëfficiënt, van de correlatie tussen de Likertwaarden en de bijbehorende rapportcijfers, van respondent 3 is 0,974542181 (zie Figuur 5). De correlatiecoëfficiënt, van de correlatie tussen de Likertwaarden en de bijbehorende rapportcijfers, van respondent 4 is 0,966668712 (zie Figuur 6).



Figuur 7: correlatie Likertwaarden en rapportcijfers van alle respondenten

Alle bovenstaande correlaties van de respondenten zijn opgenomen in Figuur 7. Hierbij is reeks1 van respondent 1, reeks2 van respondent 2, reeks3 van respondent 3 en reeks4 van respondent 4. In dit totaaloverzicht is te zien dat er een duidelijk verband is tussen de Likertwaarden en het rapportcijfer van de invloed van de desbetreffende relatie. Dit komt tevens naar voren bij de correlatiecoëfficiënten, ze liggen allen dichtbij de +1. Dit betekent dat er een positieve correlatie bestaat tussen de Likertwaarden en de rapportcijfers die de respondenten geven voor de relatie en de beïnvloeding van deze relatie op het totaal aan vertrouwen.

7 Conclusies en aanbevelingen

In dit hoofdstuk worden de conclusies weergegeven uit het onderzoek. De conclusies worden op basis van de gevonden resultaten en de analyse hiervan getrokken. Aanvullend zullen er aanbevelingen gedaan worden voor vervolgonderzoek.

7.1 Conclusies

Om vertrouwen te meten en eventueel bewust mee te sturen vanuit het risicomanagement, is het noodzakelijk om te weten of er een relatie bestaat tussen vertrouwen en ITO-risico's.

Dit onderzoek probeert een antwoord te geven op de volgende onderzoeksvragen:

- 1) In hoeverre is er een relatie tussen de factoren van trustworthiness en IT-outsourcing risico's?
- 2) Wat is de sterkte van deze relatie(s)?

De conclusies per onderzoeksvraag worden hieronder uitgewerkt.

Onderzoeksvraag 1: In hoeverre bestaat er een invloed van één of meerdere factoren van trustworthiness op de perceptie van IT-outsourcing risico's?

Gedurende het literatuuronderzoek heeft de onderzoeker de mogelijk relevante ITO-risico's gekoppeld aan de factoren van trustworthiness van Mayer, zie kolom drie van Tabel 9. Middels het empirisch onderzoek is er getoetst of de factoren van trustworthiness daadwerkelijk invloed hebben op de perceptie van ITO-risico's, zie kolom vier van Tabel 9.

Dit onderzoek geeft, op basis van een beperkte populatie, een eerste indicatie van de relaties tussen de factoren van trustworthiness en de door de onderzoeker geselecteerde ITO-risico's. De factoren die in het zwart gedrukt staan in de vierde kolom van Tabel 9 zijn de factoren waarover de respondenten eenduidig hebben geantwoord; er bestaat een relatie tussen deze factoren en het desbetreffende ITO-risico. Vanuit de overeenkomsten tussen de Likertwaarden van de respondenten komt naar voren dat de eenduidige antwoorden met betrekking tot de relatie alle vallen in categorie 1 (er bestaat een relatie). Over de andere categorieën 2 (neutraal) en 3 (er bestaat geen relatie) bestaat geen overeenstemming.

De groen gedrukte factoren in de vierde kolom van Tabel 9 zijn factoren die op basis van de analyse van de onderzoeker toch duiden op een relatie met het ITO-risico.

Tabel 9: Factoren van trustworthiness die een relatie hebben met ITO-risico's

#	ITO Risico's	Factoren van vertrouwen die invloed hebben op het ITO-risico, door de onderzoeker vastgesteld in het literatuuronderzoek	Factoren van vertrouwen die invloed hebben op het ITO-risico, vastgesteld door empirisch onderzoek
1	Backlash from internal IT staff	Integrity	Benevolence, Integrity
2	Contractual risk	Ability, Benevolence, Integrity	Ability, Benevolence, Integrity
3	Coordination between client and supplier	Ability, Benevolence, Integrity	Integrity
4	Cultural differences between client and supplier	Ability, Benevolence,	Benevolence, Integrity
5	Difficulty in managing remote teams	Benevolence, Integrity	Ability, Benevolence
6	Lack of trust	Ability, Benevolence, Integrity	Ability, Benevolence, Integrity

7	Loss of control over data	Ability, Integrity	Ability, Integrity
8	Opportunistic behaviour	Benevolence, Integrity	Benevolence, Integrity
9	Security / privacy breach	Integrity	Ability, Benevolence, Integrity
10	Shirking ¹ Goal incongruence	Integrity	Benevolence
11	Single / Double moral hazard	Integrity	Benevolence, integrity
12	Supplier employees have poor communication skills	Benevolence	Ability, Benevolence

De factor benevolence wordt tien keer gerelateerd aan een ITO-risico, integrity wordt negen keer gerelateerd aan een ITO-risico en ability zes keer. Dit maakt dat benevolence de belangrijkste factor is binnen deze twaalf ITO-risico's en integrity de tweede belangrijkste factor. Door in te zetten op het vergroten van benevolence heeft dit op de meeste ITO-risico's effect.

Van de veertien relaties waarbij geen eenduidige antwoorden zijn gegeven door de respondenten, zijn er zes relaties die betrekking hebben op de factor ability, vijf relaties die betrekking hebben op benevolence en drie op integrity. Drie relaties die betrekking hebben op benevolence zijn vanuit de analyse toch als relatie aangemerkt, zie groene tekst in kolom vier van Tabel 9. Één relatie met ability is vanuit de analyse van de onderzoeker aangemerkt als categorie 3 (er bestaat geen relatie). Hieruit kan geconcludeerd worden dat de factor ability lastiger te plaatsen is in relatie met de geselecteerde ITO-risico's en dat ability minder in relatie wordt gezien met ITO-risico's.

Drie ITO-risico's zijn dubbel betrokken bij een relatie waarover geen overeenstemming is; dit zijn 'coordination between client and supplier', 'difficulty in managing remote teams' en 'goal incongruence'. Vanuit de interviews is gebleken dat deze ITO-risico's ook lastig te relateren waren met de factoren van trustworthiness. De respondenten hebben lang over deze antwoorden nagedacht.

Van de veertien relaties waar geen eenduidig antwoord op werd gegeven door de respondenten, blijven er na de analyse van de onderzoeker nog tien relaties over, waarbij de respondenten verschillende antwoorden hebben gegeven. De populatie in dit onderzoek is te klein om een goede analyse te maken voor deze tien relaties. Deze resultaten zouden in een (groter) vervolgonderzoek meegenomen kunnen worden. Hierbij moet opgemerkt worden dat de vragen die vooraf zijn opgesteld achteraf gezien niet specifiek genoeg waren. Ondanks dat de bedoeling en richting van de vragen en het onderzoek vooraf was uitgelegd aan de respondenten, kan het zijn dat de vragen aan het eind van het interview minder duidelijk waren.

Vanuit dit onderzoek kan geconcludeerd worden dat alle ITO-risico's, die de onderzoeker vooraf heeft geselecteerd, een relatie hebben met één of meerdere factoren van trustworthiness.

Onderzoeksvraag 2: Indien er invloed is op de perceptie van ITO-risico's, hoe sterk is deze invloed?

Uit de analyse van de resultaten is naar voren gekomen dat de Likertwaarde van de relatie en het rapportcijfer van de invloed van deze relatie op het totaal aan vertrouwen correleren met elkaar. Er bestaat een positieve correlatie tussen de Likertwaarden voor de relatie en de rapportcijfers die de respondenten geven voor de beïnvloeding van deze relatie op het totaal aan vertrouwen.

Uit het onderzoek kan geconcludeerd worden dat hoe hoger de Likertwaarde, hoe hoger de beïnvloeding is van deze relatie op het totaal aan vertrouwen.

¹ In de uitvoeringsfase verschilt de lijst met ITO-risico's van de lijst zoals deze is opgesteld in het literatuuronderzoek.

7.2 Aanbevelingen voor verder onderzoek

Dit onderzoek geeft de relatie weer tussen de factoren van trustworthiness en door de onderzoeker vooraf geselecteerde ITO-risico's. Voor vervolgonderzoek in het zinvol de lijst met ITO-risico's uit te breiden, omdat de huidige lijst beperkt is en samengesteld is door middel van interpretatie van de onderzoeker. Het is dan ook niet uit te sluiten dat andere ITO-risico's eveneens een relatie hebben met de factoren van trustworthiness.

Daarnaast is dit onderzoek beperkt tot organisaties binnen de rijksoverheid, zowel aan de klantzijde als aan de leverancierszijde. Om te zorgen dat het onderzoek een representatieve afspiegeling is van verschillende type organisaties zou het onderzoek overgedaan kunnen worden bij niet-overheid organisaties.

Uit het onderzoek is naar voren gekomen dat de Likertwaarde van de relatie en het rapportcijfer voor de invloed van deze relatie op het totaal aan vertrouwen correleren met elkaar. Voor nader onderzoek zou het vragen naar rapportcijfers wellicht achterwege kunnen blijven. Het zou zinvol zijn om te onderzoeken in hoeverre het vragen naar enkel de Likertwaarden volstaat. Deze Likertschaal zou dan uitgebreid kunnen worden naar een 7-punts Likertschaal of zelfs naar een nog uitgebreidere versie van een Likertschaal. In hoeverre de correlatie die bestaat tussen de Likertwaarde en het rapportcijfer ook buiten de context van dit onderzoek aanwezig is, is een vraag die terecht gesteld kan worden. Is de correlatie specifiek tussen de desbetreffende Likertwaarden en de rapportcijfers van dit onderzoek of is de correlatie inherent aan de Likertschaal? Hier zou nader onderzoek naar gedaan moeten worden.

Naar aanleiding van de conclusies van dit onderzoek is een vervolgonderzoek naar het bewust kunnen sturen van de factoren van trustworthiness om de perceptie van de ITO-risico's te verlagen een interessante vervolgstap.

8 Reflectie

In dit hoofdstuk wordt er gereflecteerd op de kwaliteit van het onderzoek en de houdbaarheid van de conclusies.

8.1 Kwaliteit onderzoeksdata en houdbaarheid van de conclusies

Voor de kwaliteit van de onderzoeksdata is het van belang te kijken naar de betrouwbaarheid en validiteit (Saunders M., 2015). Bij dit onderzoek waren van belang:

- *Respondentenbias*: de onderzoeker heeft de indruk dat de respondenten zich tijdens het interview veilig voelden en dat zij zich open opstelden vanwege het anonimiseren van het onderzoek. Dit baseert de onderzoeker op de openheid en de antwoorden die de respondenten gaven. De onderzoeker heeft geprobeerd de toelichting van het onderzoek en de begrippen zo neutraal mogelijk te bespreken, maar voorkeuren kunnen non-verbaal of indirect overgebracht zijn. Tevens is de respondent tijdens het interview door de onderzoeker gestimuleerd tot antwoorden, doordat zij herhalingen, opmerkingen en aansporingen heeft gegeven, waardoor de respondent onbewust een bepaalde denkrichting kan zijn ingeslagen.
- *Waarnemersfouten* zijn vermoedelijk niet of nauwelijks voorgekomen. De onderzoeker heeft dit getracht te voorkomen door het structureren van de interviews en het uitwerken van de volledige antwoorden van de respondenten.
- Om de *interne validiteit* te borgen is er extra aandacht besteed aan het bespreken van de begrippen die in het interview naar voren zouden komen. Dit bleek achteraf gezien ook nodig te zijn geweest. De keuze voor het afnemen van interviews was hierdoor ook een juiste keuze, omdat middels een andere dataverzamelmethode deze toelichting niet

helder zou zijn overgekomen. Ook is er tijdens de interviews nog regelmatig teruggevallen op de lijst met begrippen ter verduidelijking.

De vragen die vooraf zijn opgesteld waren achteraf gezien niet specifiek genoeg. Ondanks dat het doel van het onderzoek en de richting van de vragen vooraf waren uitgelegd aan de respondenten, kan het zijn dat de vragen aan het eind van het interview minder duidelijk waren. De onderzoeker verwacht niet dat de strekking van de vragen niet duidelijk was voor de respondenten, omdat er continue interactie was tussen respondent en onderzoeker. Indien de vraag niet duidelijk was dan werd door de desbetreffende respondent verduidelijking gevraagd. Desalniettemin is het meer specificeren van de vraag en richting van de vraag in een vervolgonderzoek of herhaling van dit onderzoek zeer gewenst.

De respondenten zijn niet willekeurig geselecteerd, maar op basis van de relatie die zij hebben met de IT-leverancier. Het voordeel hiervan is dat zij ervaring hebben met de risico's die bestaan bij IT-outsourcing. Het risico is dat er mogelijk een vertekend beeld ontstaat, omdat de onderzoeker niet weet hoe deze relatie er in de praktijk uit ziet.

De gebruikte Likertschaal en rapportcijfers voor de beïnvloeding van de factoren op de ITO-risico's zou voor vervolgonderzoek nader onderzocht moeten worden. Uit het onderzoek is naar voren gekomen dat de Likertwaarde van de relatie en het rapportcijfer voor de invloed van deze relatie op het totaal aan vertrouwen correleren met elkaar. Voor nader onderzoek zou het vragen naar rapportcijfers wellicht achterwege kunnen blijven. In hoeverre de correlatie die bestaat tussen de Likertwaarde en het rapportcijfer ook buiten de context van dit onderzoek aanwezig is, is een vraag die terecht gesteld kan worden. Is de correlatie specifiek tussen de desbetreffende Likertwaarden en de rapportcijfers van dit onderzoek of is de correlatie inherent aan de Likertschaal? Hier zou nader onderzoek naar gedaan moeten worden.

- De *betrouwbaarheid* is geborgd door de onderzoeker door uitgebreid aandacht te besteden aan de opzet van het onderzoek, zoals weergegeven in hoofdstuk 4, waarin de gemaakte keuzes inclusief motivering worden beschreven. Verder zijn alle data, zoals gespreksverslagen, gebruikte documenten, audio-opnamen en 'ingevulde vragenlijsten' opgenomen in de appendix, zodat data door andere onderzoekers opnieuw geanalyseerd kunnen worden.
- De *generaliseerbaarheid* (externe validiteit) is laag van dit onderzoek, omdat er een populatie is van 4 respondenten. Desalniettemin is het van belang om te weten of de resultaten ook toepasbaar zijn op andere casus.

Gezien de relatief kleine populatie moeten de resultaten altijd in dat licht beoordeeld worden. Ook het feit dat de respondenten allen afkomstig zijn van organisaties die behoren tot de rijksoverheid is van belang. Wat voor een organisatie binnen de rijksoverheid geldt, hoeft niet van toepassing te zijn op een organisatie buiten de rijksoverheid.

Er zou met de resultaten vanuit dit onderzoek in de hand verder onderzoek gedaan moeten worden bij andere organisaties om de resultaten te toetsen en te kijken of ze te generaliseren zijn.

9 Dankwoord

Barry

–bedankt voor je kritische blik, eerlijke woorden en het ‘redigeren’ van mijn scriptie. Je bent mijn steun en toeverlaat. ♥

Daniël en Mara

–bedankt dat jullie zijn wie je bent. Jullie hebben een mooi hart en ik ben trots op jullie. De liefde die ik dagelijks ontvang van jullie heeft mij de kracht gegeven om dit traject af te ronden. ♥

Werner

–dank voor het begeleiden van mijn afstudeeronderzoek. Helaas hebben we het niet samen kunnen afmaken. Jouw vertrouwen tijdens het afstudeeronderzoek en onze strakke planning, heeft er voor gezorgd dat ik voor de zomer kan afstuderen!

Rob

–dank voor het kritisch meelezen en je feedback. De scriptie is er kwalitatief beter door geworden.

Respondenten

–alle respondenten wil ik hierbij bedanken voor de medewerking en de gemotiveerde antwoorden die jullie gegeven hebben. Het was niet makkelijk om de antwoorden te vinden, daar ben ik me heel erg van bewust. Dus nogmaals dank! Jullie weten zelf wie je bent, jullie moeten natuurlijk wel anoniem blijven 😊.

Anneke

–jij hebt me geleerd dat alles wat ik bedenk mogelijk is en dat ik alles waar ik van droom kan waarmaken. Bedankt Mam!

Familie, vrienden en collega's

–hierbij wil ik iedereen bedanken voor het meeleven tijdens mijn studie, het vragen hoe het met me gaat en de opbeurende woorden als ik het even niet meer zag zitten. Bedankt!

10 Referenties

- Al-Natour S, B. I., Cefetelli RT. . (2008). The effects of process and outcome similarity on users. *Decision Sciences*, 39(2), 175-211.
- Aung, Z. Z. (2008). Operational Risk Management Framework for service outsourcing: Consideration of risk dimensions and their application into the framework. *International Journal of Electronic Business Management*, 6(3), 120-130.
- Bachmann, R. (2001). Trust, Power and Control in Trans-Organizational Relations. *Organization Studies*, 22(2), 337-365.
- Bill McEvily, M. T. (2011). Measuring trust in organisational research: Review and recommendations. *Journal of trust research*, 23-63.
- Chryssochoidis G, S. A., Krystallis A. (2009). Public trust in institutions and information sources regarding risk management and communication: Towards integrating extant knowledge. *Journal of Risk Research*, 12(2), 137-185. doi:10.1080/13669870802637000
- Das, T. (2001). Trust, Control, and Risk in Strategic Alliances: An Integrated Framework. *Organization Studies*, 22(2), 251-283.
- Davis, R. C. M. a. J. H. (1999). The Effect of the Performance Appraisal System on Trust for Management: A Field Quasi-Experiment. *Journal of Applied Psychology*, 84(1), 123-136.
- Earle, T. C. (2004). Thinking aloud about trust. *Risk Analysis*, 24(1), 169-183.
- Earle, T. C. (2010). Trust in Risk Management: A Model-Based Review of Empirical Research. *Risk Analysis*, 30(4), 541-574.
- Gill, H. (2005). Antecedents of trust: Establishing a boundary condition for the relation between propensity to trust and intention to trust. *Journal of Business and Psychology*, 19(3), 287-302.
- Heiskanen, A. (2008). Control, trust, power, and the dynamics of information system outsourcing relationships: A process study of contractual software development. *Journal of Strategic Information Systems*, 17, 268-286.
- Heyns, M., & Rothmann, S. . (2015). Dimensionality of trust: An analysis of the relations between propensity, trustworthiness and trust. *A Journal of Industrial Psychology/SA Tydskrif vir Bedryfsielkunde*, 41(1263).
- Inkpen, R. B. a. A. C. (2011). Understanding Institutional- based Trust Building Processes in Inter-organizational Relationships. *Organization Studies*, 32(2), 281-301. doi:10.1177/0170840610397477
- Kadabade, A. (2000). critical review - outsourcing: a paradigm shift. *Journal of Management*, 19(8), 670-728.
- Kavan, S. M. M. a. B. (2005). Moments of governance in IS outsourcing: conceptualizing effects of contracts on value capture and creation. *Journal of Information Technology*, 20, 152-169.
- Koh, C. S., Ang Straub, Detmar W. (2004). IT Outsourcing Success: A Psychological Contract Perspective. *Information Systems Research*, 15(4), 356-373. doi:10.1287/isre.1040.0035
- Langfield-Smith, K. a. D. S. (2001). *Management and control of outsourcing relationships : Evidence from the electricity industrie*.
- Lisa M. PytlikZillig, J. A. H., Ellie Shockley, Mitchel N. Herian, Tess M.S. Neal, Christopher D. Kimbrough, Alan J. Tomkins & Brian H. Bornstein. (2016). The dimensionality of trust-relevant constructs in four institutional domains: results from confirmatory factor analyses. *Journal of Trust Research*. doi:10.1080/21515581.2016.1151359
- Mass Soldal Lund, B. S., Ketil Stolen. (2010). Evolution in Relation to Risk and Trust Management. 5, 1, 49-55.
- Mayer, R. C., Davis, J. H., & Schoorman, F. D. . (1995). An integrative model of organizational trust. *Academy of management review*. 20(3), 709-734.

Referenties:

- Nooteboom, B. (2000). Trust as a Governance Device. In M. C. a. A. Godley (Ed.), *Cultural Factors in Economic Growth* (pp. 44-68): Springer Berlin Heidelberg.
- Rosalinde Klein Woolthuis, B. H. a. B. N. (2005). Trust, Contract and Relationship Development. *Organization Studies*, 813-840.
- Rousseau, D. M. (2001). Schema, promise and mutuality: The building blocks of the psychological contract. *Journal of Occupational & Organizational Psychology*, 74(4), 511.
- Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-disipline view of trust. *Academy of Management Review*, 23(3), 393-404.
doi:10.5465/AMR.1998.926617
- Saunders, M., Lewis, P., Thornhill, A. (2015). *Methoden en technieken van onderzoek*. Amsterdam: Pearson Benelux
- Siegrist, T. C. E. a. M. (2006). Morality Information, Performance Information, and the Distinction Between Trust and Confidence. *Journal of Applied Social Psychology*, 36(2), 383-416.
- Tetteroo, J. (2016). *De risico's van IT outsourcing en IT co-sourcing vergeleken, literatuurstudie BPMIT*. Open Universiteit.
- Tomkins, C. (2001). Interdependencies, trust and information in relationships, alliances and networks. *Accounting, Organizations and Society*, 26, 161-191.
- Urbach, N., & Wurz, T. (2012). How to steer the IT outsourcing Provider. *Business & Information systems engineering*, 5, 247-259.
- Yin, R. (2003). K.(2003). *Case study research: Design and methods*. Sage Publications, Inc, 5, 11.

11 Appendices

11.1 Appendix 1: Begrippenlijst

Begrip	Definitie / omschrijving
Algemeen	
Outsourcing	Het uitbesteden van een dienst of activiteit aan een derde partij (Langfield-Smith, 2001).
Vertrouwen	Vertrouwen is een psychologische toestand die de kwetsbaarheid accepteert op basis van positieve verwachtingen van de intenties of het gedrag van een ander (Mayer, 1995).
Factors of trustworthiness (Mayer, 1995)	
Bekwaamheid (Ability)	De groep van vaardigheden, competenties en karakteristieken die het mogelijk maken invloed uit te oefenen in een specifiek domein (Mayer, 1995).
Integriteit (Integrity)	De perceptie van de vertrouwensgever dat de vertrouwde persoon een set van principes aanhoudt die voor vertrouwensgever acceptabel zijn (Mayer, 1995).
Welwillendheid (Benevolence)	De mate waarin van een vertrouwde persoon geloofd wordt dat hij het beste voorheeft met de vertrouwensgever (Mayer, 1995).
IT-outsourcing	
IT-outsourcing	Het uitbesteden van diensten en / of producten wordt ook steeds vaker toegepast in de Informatie Technologie. Hier wordt het Information Technologie Outsourcing (ITO) genoemd, wat er op neer komt dat alle IT-bezittingen, resources en activiteiten worden overgedragen aan een derde partij die dit gaat beheren (Urbach & Wurz, 2012).
ITO-risico	Een gevaar van schade of verlies binnen de IT-outsourcing.
ITO-risico's	
Backlash from internal IT staff	<p>Een backlash (tegenwerking) komt vanuit de interne IT-medewerkers. IT-werknemers binnen de eigen organisatie moeten samenwerken met werknemers van de IT-leverancier die in de toekomst mogelijk hun baan zouden kunnen overnemen, omdat de interne IT-medewerkers overbodig zijn geworden. De interne werknemers kunnen hierdoor een vijandige houding aannemen, sturen op publieke bewustwording, of proberen politieke druk uit te oefenen.</p> <p>Indien interne IT-medewerkers geconfronteerd worden met organisatie brede verplaatsing van werk (IT-outsourcing), kan een backlash ook resulteren in intellectuele verlamming, productiviteitsverlies, stress en onzekerheid onder de medewerkers (Gartner, 2003). In beide gevallen gaat het om negatieve gevolgen naar aanleiding van het mogelijk verlies van banen of werkzaamheden bij ITO.</p>
Contractual risk	Er kunnen veel problemen optreden met betrekking tot contracten, die samen

Appendices: Appendix 1: Begrippenlijst

	<p>te vatten zijn als contractuele risico's. Voorbeelden van deze risico's zijn:</p> <ul style="list-style-type: none"> • contractbreuk; • inflexibele contracten; • onenigheid omtrent de details van een contract; • contractduur; • onduidelijkheid met betrekking tot het resultaat van de door de dienstverlener uit te voeren processen; • conflicterende en ongelijke doelen.
Coordination between client and supplier	Een effectieve coördinatie tussen de klant en de ICT- dienstverlener kan een goede samenwerking vergemakkelijken. Dit zou kunnen betekenen dat een minder optimale coördinatie een negatief effect kan hebben op de samenwerking, wat als een risico gezien moet worden. Coördinatie moet hierbij gezien worden als onderlinge afstemming tussen de klant en de leverancier. Het risico is dat er onderling geen goede (of onvoldoende) afstemming is tussen klant en leverancier.
Cultural differences between client and supplier	Ondanks uitgebreide selectietrajecten, wordt het cultuurverschil tussen de partijen (klant en leverancier) vaak benoemd als een hindernis voor verbetering van de samenwerking. De culturele ('zachte') aspecten zijn vaak onderbelicht of worden overschaduwd door de 'harde' aspecten. De focus ligt nog te veel op processen, contracten en SLA's, terwijl het in de relatie met de business veel meer gaat over de ontwikkelingen die er bij de klant spelen en de wijze waarop je daarmee omgaat in de samenwerking. Hoe zorg je ervoor dat het 'DNA' matcht met dat van de organisatie?
Difficulty in managing remote teams	Dit risico is voornamelijk van toepassing op <i>offshoring</i> (outsourcing in een gebied dat ver weg ligt, bijv. India) en softwareontwikkeling met behulp van virtuele teams. Problemen die hierbij geschetst worden zijn het ontbreken van een gevoel van urgentie voor uit te voeren veranderingen door de fysieke afstand tussen teams. Tevens worden taalbarrières en culturele verschillen hierbij ook benoemd.
Goal incongruence	<p>Goal congruence betekent dat persoonlijke doelstellingen van de werknemers ook belangrijk zijn en dienen aan te sluiten bij de bedrijfsdoelstellingen. De belangen van zowel de organisatie als de werknemers moeten op één lijn komen te liggen om het beste uit de organisatie te halen. Het nastreven van de doelstellingen van de organisatie en de werknemersdoelstellingen is een goede manier om alles uit je organisatie te halen. Het tegenovergestelde van goal congruence is goal incongruence.</p> <p>Wanneer er sprake is van goal incongruence, namelijk dat niet alle neuzen één richting op staan, is dit een risico voor ITO. Indien de leverancier geen rekening houdt met de persoonlijke doelstellingen van de medewerkers van de klant is, het resultaat informatie-asymmetrie tussen klant en leverancier.</p>
Lack of trust	<p>De meest gangbare definitie van vertrouwen is:</p> <p><i>“Vertrouwen is een psychologische toestand die de kwetsbaarheid accepteert op basis van positieve verwachtingen van de intenties of het gedrag van een ander” (Mayer, 1995).</i></p> <p>Vertrouwen wordt ook wel omschreven als “geloven dat de persoon die men</p>

	<p>vertrouwt zal doen wat men van hem verwacht”. Hierbij gaat het om het algehele vertrouwen wat de klant heeft in de IT-leverancier.</p> <p>Vertrouwen is belangrijk voor het succes van IT-outsourcing. Indien dit vertrouwen ontbreekt is dit een risico voor de IT-outsourcing.</p>
Loss of control over data	<p>Verlies van data aan de concurrentie kan als een risico gezien worden. In theorie zou het kunnen voorkomen dat door verlies van controle over data, informatie van een klant bij een concurrent terecht komt. Logischerwijs vindt verlies van controle over data plaats indien bijvoorbeeld (een deel van) de infrastructuur wordt geoutsourcet naar een dienstverlener, waarbij de dienstverlener de infrastructuur overneemt. Ook als een dienstverlener vanaf een externe locatie beheer uitvoert over de systemen van de klant (of een extern datacenter heeft) kan dit risico plaatsvinden, alhoewel het risico mogelijk minder groot is door in plaats zijnde beveiligingsmaatregelen vanuit de klantorganisatie.</p>
Opportunistic behaviour	<p>Er zijn verschillende vormen van opportunistisch gedrag. In de masterthesis van Heuterman E.A. (2012) van de Vrije Universiteit Amsterdam, worden drie onderwerpen gedefinieerd: <i>shirking</i>, <i>free-riding</i> en <i>hold-up</i>.</p> <p>Shirking <i>“Shirking”</i> of <i>“Service debasement”</i> is het opzettelijk ondermaats presteren en het verlagen van de geleverde service of anders gezegd, het verlagen van de waarde, kwaliteit en / of status van de service die geleverd wordt.</p> <p>Shirking is een actieve benadering, vergelijkbaar met jezelf verplaatsen binnen een groep vrienden in een bar, waarbij je probeert te vermijden om een rondje te geven. Het vermijden van contractuele verplichtingen, focussen op de korte termijn inkomsten, het opleggen van zoveel mogelijk kosten aan de joint venture zijn zakelijke voorbeelden hiervan.</p> <p>Free-riding Free-riding is passief, eigenlijk niets meer dan wachten tot de andere partners afspraken maken en hiervan vervolgens profiteren. Dit kan gemakkelijk worden gedaan als de bijdrage van de organisatie relatief klein is en het belang van de samenwerking voor de andere partners hoog is. Het beste moment om dit te voorkomen is in de onderhandelingsfase, hetzij door een betere omschrijving van de verplichtingen van elke partij, hetzij door ervoor te zorgen dat de samenwerking hetzelfde is voor alle partners. Uiteindelijk moet je free-riders zo veel mogelijk uitsluiten.</p> <p>Hold-up Hold-up is de meest strategische aanpak en gebaseerd op het benutten van de afhankelijkheid van de partner op de alliantie. Vergelijk het met uw loodgieter die komt met extra kosten op het moment dat de watertoevoer al is stilgelegd. Partners die deze benadering gebruiken proberen in de contractuele fase afspraken open te laten. Grotere bedrijven hebben de neiging om dit te doen met (onvoorbereide) kleinere bedrijven.</p>
Security / privacy breach	<p>Dit risico heeft te maken met beveiliging en privacy gerelateerde risico's. Deze risico's staan hieronder in niet-limitatieve opsomming:</p>

	<ul style="list-style-type: none"> • Aanvallen op de verantwoordingsplicht; • Aanvallen op authenticatie; • Aanvallen op autorisatie; • Aanvallen op beschikbaarheid; • Aanvallen op vertrouwelijkheid; • Aanvallen op integriteit; • Gecompromitteerd vertrouwelijkheid van gegevens; • Gecompromitteerde gegevensbeveiliging; • Verlies van data; • Openbaarmaking van gegevens door de provider; • Host-based aanvallen; • Onvoldoende verantwoording van de uitgevoerde acties; • Onvoldoende bescherming van persoonsgegevens; • Onvoldoende scheiding van naast elkaar bestaande gebruikers; • Verlies van vertrouwelijkheid; • Verlies van integriteit; • Misbruik van gegevens door de provider; • Netwerk-gebaseerde aanvallen; • Onbeschermde gevoelige gegevens in de transmissie en opslag. <p>Als voorbeeld: een onbeveiligde USB-stick van de klant kan door een ITO-medewerker worden meegenomen en ITO-medewerkers zouden gevoelige gegevens naar een concurrent van de klant kunnen lekken.</p>
Single / Double moral hazard	<p>Moral hazard (Nederlandse termen zijn moreel risico, moreel gevaar en moreel wangedrag) is een economisch begrip dat verwijst naar veranderingen in het gedrag van partijen indien zij niet direct risico lopen voor hun daden.</p> <p>In ITO-overeenkomsten zijn er altijd twee partijen: de klant en de dienstverlener. Een klant kan zaken doen met meerdere dienstverleners en vice versa, maar in de basis komt het neer op twee partijen die een overeenkomst met elkaar hebben afgesloten. Wanneer één van deze partijen zich niet optimaal inzet wordt dit een single moral hazard genoemd (Elitzur et al., 2012).</p> <p>IT-outsourcing wordt gekenmerkt door de samenwerking tussen twee partijen waarbij beide partijen inspanning uitoefenen, dit niet waarneembaar is voor de andere partij. Dit kan uitmonden in een situatie waarbij er geen informatie wordt uitgewisseld terwijl dit wel relevant zou zijn. Aangezien de kwaliteit van het resulterende systeem afhankelijk is van de inspanning die beide partijen leveren kan dit leiden tot informatie asymmetrie, deze situatie wordt gekenmerkt als een <i>double moral hazard</i> (Elitzur et al., 2012).</p>
Supplier employees have poor communication skills	<p>Bij dit risico gaat het over de communicatieve vaardigheden van de medewerkers van de leverancier. Indien deze vaardigheden ondermaats zijn, kan dit een risico vormen voor de samenwerking. Medewerkers van de IT-leverancier moeten communiceren met de klant. Wanneer dit niet op de juiste en een nette manier gebeurt kan hier miscommunicatie en zelfs schade door ontstaan.</p>

1.1 Appendix 2: Literatuurstudierapport

Het beïnvloeden van factoren van vertrouwen om te sturen bij outsourcen van IT

Kunnen factoren van vertrouwen ingezet worden om de kans en impact van risico's te reduceren binnen je risicomanagement bij het outsourcen van IT

Cursus:	IM060X Voorbereiden Afstuderen BPMIT
Student:	Leonie Hendriks
Identiteitsnummer:	851199058
Datum rapport:	11 december 2016
Versie nummer:	2.0
Status:	concept
Datum einde inschrijving:	02-05-2017

Influencing factors of trust to control outsourcing IT

Can factors of trust be used to reduce the likelihood and impact of risks within your risk management by outsourcing IT?

Opleiding:	Open Universiteit, faculteit Management, Science & Technology Master opleiding Business Process Management & IT
Programme:	Open University of the Netherlands, faculty of Management, Science & Technology Master Business Process Management & IT
Cursus:	IM060X Voorbereiden Afstuderen BPMIT
Student:	Leonie Hendriks
Identiteitsnummer:	851199058
Datum:	11 december 2016
Afstudeerbegeleider	Werner Rutten
Meelezer	Rob Kusters
Derde beoordelaar	nvt

Samenvatting

Vertrouwen is een veel onderzocht onderwerp binnen de sociale – en psychologische wetenschap. Ook zakelijk gedrag wordt steeds meer getracht te verklaren door middel van vertrouwen. Wat zijn de factoren van vertrouwen en hoe worden deze gemeten? Vanuit de zakelijke hoek is het interessant om te kijken of er bewust met factoren van vertrouwen gestuurd kan worden. Kan de perceptie van gedefinieerde risico's binnen IT-outsourcing hiermee gereduceerd worden? In dit literatuuronderzoek wordt antwoord gegeven op de bovenstaande vragen. Middels een beperkt literatuuronderzoek, waarbij 27 artikelen zijn onderzocht is er inzicht gegeven in de relatie tussen vertrouwen, IT-outsourcing en de risico's van IT-outsourcing.

Een voorlopige conclusie is dat, door middel van beïnvloeding van de drie factoren van vertrouwen: integriteit, welwillendheid en bekwaamheid, benoemd door Mayer, de betrouwbaarheid vergroot kan worden van een partij. Dit geldt zowel vanuit de klantzijde als vanuit de leverancierszijde.

Tevens is een belangrijke conclusie dat er veel binnen de literatuur is onderzocht met betrekking tot vertrouwen en risico management, maar dat dit literatuuronderzoek niets heeft gevonden over het *bewust* sturen van factoren van vertrouwen. Omdat dit nog niet duidelijk naar voren is gekomen binnen dit literatuuronderzoek is dit een reden voor nader onderzoek.

Trefwoorden: Vertrouwen, IT outsourcing, risicomanagement, sturen, literatuuronderzoek

Summary

Trust is a frequently studied concept within the social - and psychological science. Business behavior is also increasingly attempted to be explained by trust. What are the factors of trust and how are they measured? From a business point of view, it is interesting to see whether an organization can consciously control by factors of trust. Can the perception of defined risks within IT outsourcing be reduced by trust?

This literature research provides answers to the above questions. Through a limited literature study in which 25 items have been studied has this research given insight into the relationship between trust, IT Outsourcing and risks of IT outsourcing.

A preliminary conclusion is that, through the influence of the three factors of trust: integrity, benevolence and competence, appointed by Mayer, trustworthiness can be increased. This applies to both the client side as from the supplier side.

Another important conclusion is that there are a lot of studies on trust and risk management, but this literature research has found nothing about explicitly controlling factors of trust to reduce risks. Because this is not yet clearly emerged in the literature, this is a reason for further research.

Keywords: Trust, IT outsourcing, risk management, control, steer, literature review

Inhoudsopgave

1.	Introductie	1
1.1.	Inleiding	1
1.1.1.	Leeswijzer	1
1.2.	Context	2
1.3.	Probleemstelling	3
1.4.	Relevantie	3
1.4.1.	Praktische relevantie	3
1.4.2.	Wetenschappelijke relevantie	4
1.5.	Opdrachtformulering	4
2.	Onderzoeksaanpak	5
2.1.	Onderzoeksvragen	5
2.2.	Onderzoekstechniek en onderzoeksmethode	6
2.3.	Zoekstrategie	6
3.	Uitvoering	7
3.1.	Zoekproces	8
3.1.1.	Onderzoeksvraag 7: Is er een verband tussen risicomanagement en vertrouwen?	8
3.1.2.	Onderzoeksvraag 5: Welke rol speelt vertrouwen bij vastlegging van afspraken tussen partijen?	9
3.1.3.	Onderzoeksvraag 6: Welke indicatoren van vertrouwen bestaan er vanuit de literatuur?	10
3.1.4.	Onderzoeksvraag 8: Op welke manier kan vertrouwen ingezet worden en hoe kan dit gemeten worden binnen IT-outsourcing?	10
3.2.	Overzicht gebruikte literatuur	11
3.3.	Relevantie van de artikelen	11
4.	Resultaten	12
4.1.	Wat wordt verstaan onder vertrouwen?	12
4.1.1.	Wat is de definitie van vertrouwen	12
4.1.2.	Welke soorten vertrouwen bestaan er die van toepassing kunnen zijn op de onderzoeksvraag?	13
4.1.3.	Hoe kun je vertrouwen beïnvloeden?	14
4.1.4.	Samenvatting	14
4.2.	Welke relaties bestaan er tussen organisaties?	15
4.2.1.	Is het vertrouwen tussen organisaties anders dan tussen individuen?	15
4.2.2.	Hoe ontwikkelt de relatie tussen leverancier en klant (of organisaties)?	15
4.2.3.	Samenvatting	16
4.3.	Wat wordt verstaan onder risicomanagement?	16

4.3.1.	Wat is de definitie van risicomanagement?	16
4.3.2.	Welke soorten risico's zijn er te onderscheiden en welke is van toepassing op de onderzoeksvraag?	17
4.3.3.	Samenvatting	18
4.4.	Wat zijn de risico's bij het outsourcen van IT?	18
4.4.1.	Wat wordt verstaan onder outsourcen van IT?	18
4.4.2.	Wat zijn de voor en nadelen van IT-outsourcing?	19
4.4.3.	Wat zijn de risico's van IT-outsourcing?	19
4.4.4.	Samenvatting	20
4.5.	Welke rol speelt vertrouwen bij vastlegging van afspraken tussen partijen?	20
4.5.1.	Op welke manieren worden afspraken vastgelegd tussen organisaties	20
4.5.2.	Is er een verband tussen het vastleggen van afspraken en vertrouwen tussen partijen?	22
4.5.3.	Samenvatting	22
4.6.	Welke indicatoren van vertrouwen bestaan er vanuit de literatuur?	23
4.6.1.	Wat is er in de literatuur bekend over factoren van vertrouwen die een rol spelen bij outsourcen van IT	23
4.6.2.	Wat is de definitie van deze indicatoren	24
4.6.3.	Samenvatting	26
4.7.	Is er een verband tussen risicomanagement en vertrouwen?	26
4.7.1.	Bestaan er onderzoeken naar de verbanden tussen risicomanagement en vertrouwen?	26
4.8.	Op welke manier kan vertrouwen ingezet worden en hoe kan dit gemeten worden binnen IT-outsourcing?	27
4.8.1.	Zijn er modellen om onderzoek te doen naar vertrouwen binnen risicomanagement?	27
4.8.2.	Zijn er modellen waarmee het vertrouwen gemeten kan worden?	28
4.8.3.	Samenvatting Modellen	28
4.9.	Risico's van IT-Outsourcing die verband houden met Trustworthiness	29
5.	Conclusies	31
5.1.	Conclusie literatuuronderzoek	31
5.2.	Voortuitblik voor het empirisch onderzoek	32
6.	Referenties	33
7.	Bijlagen	35
7.1.	Bijlage 1: Lijst van tertiaire bronnen waarbinnen gezocht is	35
7.2.	Bijlage 2: overzicht gebruikte artikelen, tijdvakken, aantal keren geciteerd en bron	36
7.3.	Bijlage 3: Resultaten risicoanalyse	38
7.4.	Bijlage 4: verantwoording selectiekeuze ITO risico's in verband met vertrouwen	39
7.5.	Bijlage 5: Dimensies van Vertrouwen	44
7.6.	Bijlage 6: Modellen van vertrouwen binnen risicomanagement	45
7.7.	Bijlage 7: Onderzoek naar meten van vertrouwen	

1. Introductie

1.1 Inleiding

De afgelopen 25 jaar heeft het outsourcen van IT een enorme vlucht genomen. Waar eerst alles “in huis” werd gehouden, worden nu steeds meer delen van de bedrijfsvoering uitbesteed aan andere organisaties die in die desbetreffende werkzaamheden gespecialiseerd zijn.

In het uitbesteden van kritieke IT systemen van je onderneming creëert men een grote afhankelijkheid. Want wat gebeurt er als het mis gaat, wat betekent dit voor de continuïteit, beschikbaarheid en integriteit van de gegevens en de informatiesystemen van de onderneming?

Het uitbesteden van (delen van) IT brengt voordelen, nadelen en risico met zich mee.

In het kader van IT-outsourcing, kunnen verschillende soorten risico's worden geïdentificeerd, zoals de strategische, operationele, financiële, juridische en contractuele risico's. Risicomanagement heeft betrekking op de identificatie, mitigatie, communicatie en controle van deze soorten risico's (Lisa M. PytlikZillig, 2016; Urbach & Wurz, 2012).

Bij het uitbesteden van IT neemt men dus risico's, waarbij de kans dat ze ontstaan zo laag mogelijk gehouden moeten worden en de impact ook laag is. Hiervoor zullen maatregelen genomen moeten worden.

Het zakelijk gedrag wordt steeds meer getracht te verklaren middels vertrouwen (Earle, 2004). Kunnen factoren van vertrouwen als maatregel worden gebruikt om de perceptie van deze risico's, ook bij de relatie met een outsourcing partner, te reduceren.

Uit onderzoek naar kenmerken van relaties en hun invloed op het succes van outsourcing, blijkt duidelijk dat bepaalde relationele kenmerken (bijvoorbeeld de volledigheid van het formele contract, de perceptie van de kwaliteit van de dienstverlening, vertrouwen en flexibiliteit) positief correleren met het succes van outsourcing. Vandaar dat naast de strategische beslissing van wat er uitbesteed zal worden, de operationele sturing van deze relatie kenmerken er voor kunnen zorgen dat het outsourcing traject een succes wordt. (Urbach & Wurz, 2012).

Dit onderzoek richt zich op de vraag of er gestuurd kan worden in het zakelijk gedrag, door te sturen op factoren van vertrouwen, binnen een IT-outsourcing traject.

1.1.1 Leeswijzer

Dit document is als volgt opgebouwd:

Hoofdstuk 1 bevat de context waarbinnen dit onderzoek is uitgevoerd, de probleemstelling, de relevantie van dit onderzoek en de uiteindelijke opdrachtformulering.

Hoofdstuk 2 bevat de onderzoeksaanpak die is uitgewerkt in onderzoeksvragen die opgesteld zijn om richting te geven aan het literatuuronderzoek. Daarnaast zijn de onderzoekstechnieken en onderzoeksmethoden hier uitgewerkt alsmede de zoekstrategie.

Hoofdstuk 3 bevat de daadwerkelijke uitvoering van het literatuuronderzoek. Verder bevat dit hoofdstuk een overzicht van de gebruikte literatuur en geeft een verantwoording van de relevantie van de gebruikte literatuur in dit onderzoek.

Hoofdstuk 4 bevat de resultaten van de literatuurstudie. Specifiek gaat dit hoofdstuk in op de theorie gerelateerd aan vertrouwen, risicomanagement, IT-outsourcing en de relatie daartussen.

Hoofdstuk 5 bevat de conclusies van het literatuuronderzoek. Hier staan de belangrijkste conclusies van het onderzoek en een aanzet voor vervolgonderzoek.

1.2 Context

Dit onderzoek vindt plaats binnen het gebied van IT-outsourcing, risicomanagement en vertrouwen. Binnen deze gebieden worden een aantal basis definities gebruikt die hieronder worden weergegeven.

Outsourcen wordt gedefinieerd als:

Het uitbesteden van een dienst of activiteit aan een derde partij (Langfield-Smith, 2001).

Outsourcing wordt steeds meer toegepast, niet alleen voor de productieactiviteiten, maar ook steeds meer de traditionele in-house activiteiten zoals administratieve en management functies, inclusief de verwerking van gegevens en IT-activiteiten, human resource management services, accounting functies, interne audit en marketing (Chalos, 1995)(Langfield-Smith, 2001).

De omvang en de kosten van de diensten en / of producten zijn voor veel organisaties van invloed om steeds meer gericht te zijn op de uitbesteding van deze diensten en / of producten. The Boston Consulting Group (1991) heeft onderzoek gedaan naar meer dan 100 belangrijke bedrijven met uitgebreide outsourcing en concludeerde dat de meeste westerse bedrijven in de eerste plaats uitbesteden om te besparen op overhead of induceren op korte termijn kostenbesparingen (Kadabadse, 2000).

Het uitbesteden van diensten en / of producten wordt ook steeds vaker toegepast in de Informatie Technologie. Hier wordt het Information Technologie Outsourcing (ITO) genoemd, wat er op neer komt dat alle IT-bezittingen, resources en activiteiten worden overgedragen aan een derde partij die dit gaat beheren.

Er gaat normaal gesproken een heel proces aan vooraf voordat er gekozen wordt voor een partij die voldoet aan de eisen.

Hierbij hoort vaak ook een risicoanalyse, waarbij naast de risico's ook de voor – en nadelen worden beschreven van het outsourcen van de IT.

Naast objectieve indicatoren bestaan er ook “zachtere” indicatoren waarop gestuurd kan worden tijdens de risico analyse.

Vertrouwen is een van deze “zachtere” indicatoren die de laatste jaren veelvuldig is onderzocht binnen diverse disciplines.

Ook is vertrouwen (Trust) een centraal begrip aan het worden in het verklaren van zakelijk gedrag in de organisatorische context (Earle, 2004).

In de literatuur wordt aan het woord “vertrouwen” verschillende betekenissen gegeven. Zo is er ook in de Engelse taal een verschil in de vertaling van vertrouwen. Wat is het verschil tussen Confidence en Trust? En welke indicatoren horen hierbij? Dit wordt in hoofdstuk 4 verder uitgewerkt.

De standaard van risicomanagement, ISO 31000, definieert risico management als:

“Gecoördineerde activiteiten om het risico van de organisatie te sturen en controleren, gedefinieerd als een combinatie van de gevolgen van een gebeurtenis en de bijbehorende kans. Het risico management proces wordt gedefinieerd als de systematische toepassing van het management beleid, de procedures, activiteiten m.b.t. het communiceren , raadplegen, vaststellen van de

context, en het identificeren , analyseren, evalueren, behandeling , monitoring, en reviewen van het risico” (ISO Guide 73:2009, definitie 2.1).

1.3 Probleemstelling

Vertrouwen is iets dat bestaat tussen twee of meerdere personen, en het betreft een gevoelskwestie. Echter is het vertrouwen van de ene persoon niet hetzelfde als het vertrouwen van de andere persoon. Vertrouwen is een subjectief begrip, maar toch hebben onderzoekers in de sociale- als psychologische hoek getracht dit te onderzoeken aan de hand van indicatoren (Earle, 2004, 2010; Gill, 2005).

Uit de literatuur blijkt dat de factoren van trust correleren met hoe betrouwbaar iemand gevonden wordt (Gill, 2005).

Daarnaast wordt gesteld dat hoe hoger het vertrouwen is hoe lager de perceptie van de gedefinieerde risico's (Nooteboom, 2000).

Bij het outsourcen van IT komen diverse risico's naar voren die zo laag mogelijk gehouden moeten worden. Door het beïnvloeden van factoren van vertrouwen kan de perceptie van gedefinieerde risico's bijgesteld worden. Dat beïnvloeden gebeurt al dan niet bewust. Maar kan hier dan ook op gestuurd worden, kunnen deze factoren bewust beïnvloed worden? Hoe kan door het bewust beïnvloeden van de factoren van vertrouwen de perceptie van gedefinieerde risico's gereduceerd worden?

1.4 Relevantie

1.4.1 Praktische relevantie

Indien factoren van vertrouwen als “instrument” ingezet kunnen worden om de perceptie van risico's te reduceren kan dit in het voordeel werken voor zowel de outsourcende partij als de leverende partij. Beide richtingen worden in dit stadium van het onderzoek open gehouden.

Als klant kun je binnen je risicomanagement de perceptie van de gedefinieerde risico's verminderen door te kijken naar leveranciers die je “vertrouwt”. De klant kan op basis van de factoren van vertrouwen beoordelen of deze de leverancier vertrouwt, er vertrouwen bestaat tussen beide organisaties of eventueel zou kunnen ontstaan.

Om als leverende partij een klant binnen te halen en te binden kunnen er factoren die vertrouwen oproepen ingezet worden om invloed uit te oefenen op het risicomanagement van de klant. Dit kan door middel van verschillende factoren. Hiermee kan de leverancier zich focussen op de vraag: “Hoe ben je een betrouwbare partner voor de klant”.

1.4.2. Wetenschappelijke relevantie

In de literatuur is het bewust sturen van factoren van vertrouwen om risico's te reduceren nog niet voldoende onderzocht. Er is veel onderzocht met betrekking tot vertrouwen en risico management, maar binnen dit onderzoek is er niets gevonden over het bewust sturen van factoren van vertrouwen. Onderzoek hiernaar zou een interessante aanvulling kunnen zijn op de bestaande literatuur met betrekking tot vertrouwen, IT-outsourcing en de risico's hiervan. Indien bewust gestuurd kan worden op factoren van vertrouwen ontstaan er meer inzichten in de werking tussen sociale psychologische componenten en het maken van zakelijke keuzes.

1.5 Opdrachtformulering

Zoals in de probleemstelling al benoemd is wordt zakelijk gedrag steeds meer getracht te verklaren middels vertrouwen, daarbij rijst de vraag of er dan ook gestuurd zou kunnen worden in het zakelijk gedrag door middel van beïnvloeding van factoren van vertrouwen? Oftewel hoe kan de perceptie van de risico's, gedefinieerd binnen je risicomanagement, gereduceerd worden door te sturen op factoren van vertrouwen?

Vanuit de literatuur komt naar voren dat indien het vertrouwen tussen partijen hoog is, de risico's lager worden ingeschat (Das, 2001).

Vanuit de probleemstelling en de relevantie kan de onderstaande hoofdvraag van dit theoretische (fundamenteel) onderzoek beschreven worden:

Hoe kunnen factoren van vertrouwen bewust ingezet worden om de perceptie van de risico's van IT-outsourcing te verlagen.

Als de perceptie van het risico lager is wordt de kans dat het risico zich voordoet lager ingeschat, omdat het effect niet kan veranderen ($\text{impact} = \text{kans} * \text{effect}$). De inschatting van de kans is altijd een perceptie van een persoon.

Kunnen factoren van vertrouwen bewust ingezet worden om de perceptie, en dus de kans en impact, van gedefinieerde risico's te reduceren binnen je risicomanagement bij het outsourcen van IT met als doel om hierop te sturen.

Hierbij moeten, middels dit literatuuronderzoek antwoorden komen op de onderstaande deelvragen:

Wat wordt verstaan onder vertrouwen?

Welke relaties bestaan er tussen organisaties?

Wat wordt verstaan onder risicomanagement?

Wat zijn de risico's bij het outsourcen van IT?

Welke rol speelt vertrouwen bij vastlegging van afspraken tussen partijen?

Welke indicatoren van vertrouwen bestaan er vanuit de literatuur?

Is er een verband tussen risicomanagement en vertrouwen?

Op welke manier kan vertrouwen ingezet worden en hoe kan dit gemeten worden binnen IT-outsourcing?

2. Onderzoeksaanpak

2.1 Onderzoeksvragen

Voor het opbouwen van het theoretisch kader is een aantal onderzoeksvragen geformuleerd. Deze onderzoeksvragen zijn opgesteld om een antwoord te krijgen op de context en op de hoofdvraag en zijn onder te verdelen in onderzoeksvragen per deelvraag. Onderzoeksvraag 1, 2, 3, 4, en 6 zijn de vragen voor de context en om definities helder te krijgen. De onderzoeksvragen 5, 7 en 8 zijn de onderzoeksvragen om een antwoord op de hoofdvraag te krijgen.

1. *Wat wordt verstaan onder vertrouwen?*

- Wat is de definitie van vertrouwen?
- Welke soorten vertrouwen bestaan er die van toepassing kunnen zijn op de onderzoeksvraag?
- Hoe kun je vertrouwen beïnvloeden?

2. Welke relaties bestaan er tussen organisaties?

- Is het vertrouwen tussen organisaties anders dan tussen individuen?
- Hoe ontwikkelt de relatie tussen organisaties zich?

3. Wat wordt verstaan onder risicomanagement?

- Wat is de definitie van risicomanagement?
- Welke soorten risico's zijn er te onderscheiden en welke is van toepassing op de onderzoeksvraag?

4. Wat zijn de risico's bij het outsourcen van IT?

- Wat wordt verstaan onder outsourcen
- Wat zijn de voor en nadelen van IT-outsourcing?
- Wat zijn de risico's van IT-outsourcing?

5. Welke rol speelt vertrouwen bij vastlegging van afspraken tussen partijen?

- Op welke manieren worden afspraken vastgelegd tussen organisaties?
- Is er een verband tussen het vastleggen van afspraken en vertrouwen tussen partijen?

6. Welke indicatoren van vertrouwen bestaan er vanuit de literatuur?

- Wat is er in de literatuur bekend over factoren van vertrouwen die een rol spelen bij outsourcen van IT?
- Wat is de definitie van deze indicatoren?

7. Is er een verband tussen risicomanagement en vertrouwen?

- Bestaan er onderzoeken naar de verbanden tussen risicomanagement en vertrouwen?

8. Op welke manier kan vertrouwen ingezet worden en hoe kan dit gemeten worden binnen IT-outsourcing?

- Zijn er modellen om onderzoek te doen naar vertrouwen binnen risicomanagement?
- Zijn er modellen waarmee het vertrouwen gemeten kan worden?

2.2 Onderzoekstechniek en onderzoeksmethode

Per deelvraag is vastgesteld met welke onderzoekstechniek, onderzoeksmethode en bronnen er antwoord verkregen kan worden op de onderzoeksvraag. Deze onderzoekstechnieken, onderzoeksmethoden en bronnen zijn hieronder schematisch weergegeven.

Tabel 1: *Onderzoekstechnieken en onderzoeksmethoden*

Deelvraag	Onderzoekstechniek	Onderzoeksmethode	Soorten bronnen
<i>Wat wordt verstaan onder vertrouwen?</i>	Kwalitatief onderzoek	Literatuuronderzoek	Literatuur
<i>Welke relaties bestaan er tussen organisaties?</i>	Kwalitatief onderzoek	Literatuuronderzoek	Literatuur
<i>Wat wordt verstaan onder risicomanagement?</i>	Kwalitatief onderzoek	Literatuuronderzoek	Literatuur
<i>Wat zijn de risico's bij het outsourcen van IT?</i>	Kwalitatief onderzoek	Literatuuronderzoek	Literatuur
<i>Welke rol speelt vertrouwen bij vastlegging van afspraken tussen partijen?</i>	Kwalitatief onderzoek	Literatuuronderzoek	Literatuur
<i>welke indicatoren van vertrouwen bestaan er vanuit de literatuur?</i>	Kwalitatief onderzoek	Literatuuronderzoek	Literatuur
<i>Is er een verband tussen risicomanagement en vertrouwen?</i>	Kwalitatief onderzoek	Literatuuronderzoek interview / survey	Literatuur / onderzoek
<i>Op welke manier kan vertrouwen ingezet worden en hoe kan dit gemeten worden binnen IT-outsourcing?</i>	Kwalitatief onderzoek	Literatuuronderzoek interview / survey	Literatuur / onderzoek

2.3 Zoekstrategie

Voor dit onderzoek wordt gebruik gemaakt van de literatuurbronnen zoals deze aangeboden worden op de "Digitale Bibliotheek" van de Open Universiteit. Hierbij wordt gezocht binnen alle disciplines, omdat het begrip "Vertrouwen" verder rijkt dan de discipline "managementwetenschappen". De lijst van bronnen waarbinnen wordt gezocht is opgenomen in Bijlage 1.

Om een zo scherp mogelijke set van artikelen te verkrijgen zijn onderstaande keywords (Engels en Nederlands) samengesteld waarop wordt gezocht:

- Riskmanagement / Risicomanagement
- Trust, Confidence/ Vertrouwen
- Trustworthiness / betrouwbaarheid
- Factors / factoren
- Antecedents
- Organizational Trust / Organisatie vertrouwen
- Organisational Trust / Organisatie vertrouwen
- Relationship / Relatie
- Organisation / Organisatie
- Organization / Organisatie
- Business / Bedrijf

- IT Outsourcing
- Risks / Risico's
- Control / Sturen
- Steer / Sturen
- Definition / Definitie
- Contract

In hoofdstuk 3 zijn de samengestelde query's opgenomen, waarop per onderzoeksvraag is gezocht .

Aanvullende opmerkingen:

- De genoemde keywords zijn zowel zelfstandig (bijvoorbeeld Trust) als in combinatie met elkaar gebruikt (bijvoorbeeld Trust + organisation).
- Bij dit literatuuronderzoek is er voornamelijk gezocht naar Engelstalige literatuur en in beperkte mate naar Nederlandstalige literatuur.
- Bij het selecteren van de keywords is rekening gehouden met zowel de Britse als de Amerikaanse spelling.
- Bij het zoeken naar literatuur wordt niet ingeperkt op datum van publicatie.
- De resultaten van de literatuurstudie worden beheerd met behulp van Endnote, bibliografische software van Reuters.
- In de uitwerking van dit onderzoek zullen Engelse kreten en terminologie gebruikt worden aangezien er in het Nederlands niet altijd de juiste vertaling voor te vinden is.

Tijdens de oriëntatie naar het onderzoeksonderwerp zijn er twee belangrijke review artikelen naar voren gekomen. Aan de hand van deze twee artikelen wordt tevens de sneeuwbalmethode toegepast om te zoeken naar artikelen waarna gerefereerd wordt in de teksten. De sneeuwbalmethode zal ook toegepast worden op andere relevante artikelen.

3. Uitvoering

Aan de hand van de trefwoorden die vooraf zijn opgesteld is er gezocht in tertiaire bronnen, waarbij naar literatuur is gezocht die op een verantwoorde wijze tot stand zijn gekomen. (Saunders M., 2015) Dat wil zeggen dat alleen gezocht is naar peer-reviewed artikelen gepubliceerd in wetenschappelijke journals en proceedings. De artikelen die gevonden zijn op basis van de trefwoorden zijn in eerste instantie gefilterd door een snelle lezing van de samenvatting en inhoud. Artikelen zijn geselecteerd voor dit onderzoek wanneer de inhoud van het artikel ingaat op de thematiek van een deelvraag en bijdraagt aan de beantwoording van de deelvragen geformuleerd voor het literatuur onderzoek.

3.1 Zoekproces

Het zoekproces heeft volgens de onderstaande stappen plaatsgevonden:

Start zoekopdracht

Keywords en query's in google Scholar en OU database;

Scannen titels en een snelle scan op inhoud;

Nieuwe query's opstellen aan de hand van gevonden artikelen;

Nieuwe query's door google Scholar en OU database;

Scannen titels en een snelle scan op inhoud;

Selectie van artikelen;

Opstellen definitieve literatuuroverzicht.

Einde zoekopdracht

De vooraf gedefinieerde keywords zijn gebruikt om de definities en de context helder te krijgen van dit literatuuronderzoek, dit zijn de onderzoeksvragen 1 tot en met 3.

Onderzoeksvraag 4 (*Wat zijn de risico's bij het outsourcen van IT?*) is beantwoord door middel van een literatuuronderzoek gedaan door J. Tetteroo, naar de risico's van IT-outsourcing. In afstemming met de begeleider van dit onderzoek, is het onderzoek van Tetteroo voldoende bevonden om de risico's van IT-Outsourcing aan te geven, en als zodanig te gebruiken voor dit onderzoek.

Om de kernvragen van dit onderzoek en de onderzoeksvraag te beantwoorden (vraag 5,6,7 en 8) zijn de onderstaande query's gebruikt.

De onderzoeker is begonnen met query's te maken voor onderzoeksvraag 7, daarna onderzoeksvraag 5, onderzoeksvraag 6 en als laatste onderzoeksvraag 8. De reden dat er is begonnen met onderzoeksvraag 7 is een bewuste keuze van de onderzoeker. De onderzoeker wilde in eerste instantie onderzoeken of er al bestaande onderzoeken en verbanden waren tussen risicomanagement en vertrouwen. Indien dit het geval zou zijn dan konden de onderzoeksvragen 5 en 6 vandaaruit beantwoord worden.

De artikelen die gevonden zijn bij de verschillende query's en de onderzoeksvragen konden in een aantal gevallen ook gebruikt worden om andere onderzoeksvragen te beantwoorden.

3.1.1 Onderzoeksvraag 7: Is er een verband tussen risicomanagement en vertrouwen?

Opmerking van de onderzoeker: Voor de duidelijkheid is in dit verslag bij de query's aangegeven dat er gezocht is met AND, echter in de daadwerkelijke query in Google scholar is dit achterwege gelaten aangezien dit al in de techniek van google scholar zit. Vanwege dit feit staat de AND in de query's tussen haakjes.

Om onderzoeksvraag 7 te beantwoorden is de volgende query opgesteld:

allintitle: trust (AND) risk (AND) management

Deze query leverde 230 resultaten op. Om deze set van artikelen kleiner te maken is gekozen om het woord "in" toe te voegen aan de Query. De onderzoeker heeft hiervoor gekozen, omdat bij de beoordeling van de titels van de artikelen en een snelle scan van de inhoud van de gevonden artikelen de inhoud hiervan niet overeen kwam met de onderzoeksvraag. De onderzoeksvraag richt zich meer op Trust die binnen het risicomanagement wordt gebruikt als maatregel om bewust te sturen op een lagere perceptie van het risico.

Deze query is vervolgens aangescherpt met de volgende query:

allintitle: trust (AND) in (AND) risk (AND) management,

Deze query leverde 124 resultaten op. In de resultaten kwam Timothy C. Earle veelvuldig naar voren en zijn artikelen zijn ook veel geciteerd. Aan de hand van de literatuurlijst die Earle had bij zijn artikelen zijn de relevante artikelen gezocht aan de hand van de sneeuwbalmethode. De 124 resultaten zijn verder gescand op titel en inhoud.

In "Thinking Aloud about Trust: A Protocol Analysis of Trust in Risk Management" van Earle is een definitie genoemd van Trust door Rousseau. Het artikel waar naar verwezen is in dit artikel, is vervolgens onderzocht en als vervolg is er gezocht naar meerdere artikelen die geschreven zijn door Denise M. Rousseau.

Denise M. Rousseau blijkt een veel geciteerd onderzoeker te zijn en de volgende twee artikelen zijn vervolgens geselecteerd (op basis van relevantie en passende bij de onderzoeksvraag):

Not so different after all: A cross-discipline view of trust (7492 geciteerd).

Schema, promise and mutuality: The building blocks of the psychological contract, (916 keer geciteerd).

3.1.2 Onderzoeksvraag 5: Welke rol speelt vertrouwen bij vastlegging van afspraken tussen partijen?

Om onderzoeksvraag 5 te beantwoorden is er verder gekeken naar de artikelen van Rousseau die het begrip psychologisch contract beschrijft in haar artikelen.

Er is gekeken welke begrippen Rousseau gebruikt in de relevante artikelen over het psychologisch contract.

Op basis van deze begrippen die Rousseau hanteert in haar artikelen is door de onderzoeker een nieuwe query gemaakt om te onderzoeken of er meer literatuur is over het psychologisch contract in combinatie met Trust.

allintitle: trust (AND) psychological (AND) contract

Deze query gaf 73 resultaten die de onderzoeker heeft bekeken en een selectie hieruit heeft gemaakt op basis van titel, waarna een snelle scan van inhoud is toegepast. In deze bekeken resultaten werd Rousseau erg veel geciteerd en daarom is gekozen om de twee geselecteerde artikelen van Rousseau bij de zoekvraag van onderzoeksvraag 7, te gebruiken om onderzoeksvraag 5 te beantwoorden.

3.1.3 Onderzoeksvraag 6: Welke indicatoren van vertrouwen bestaan er vanuit de literatuur?

Om onderzoeksvraag 6 te beantwoorden zijn de volgende query's gebruikt:

allintitle: organizational (AND) trust

allintitle: organisational (AND) trust

De eerste query gaf 2380 hits, echter direct boven aan stond het artikel van Mayer, An Integrative Model of Organizational Trust. Dit artikel is 14699 keer geciteerd. Dit artikel viel de onderzoeker op omdat dit artikel ook al was geciteerd door Rousseau en Earle.

Omdat Mayer zo vaak is geciteerd heeft de onderzoeker dit artikel geselecteerd.

De query (**allintitle: trust (AND) in (AND) risk (AND) management**) waarmee onderzoeksvraag 7 tevens is beantwoord geeft ook resultaten van artikelen waarmee onderzoeksvraag 6 beantwoord kan worden.

3.1.4 Onderzoeksvraag 8: Op welke manier kan vertrouwen ingezet worden en hoe kan dit gemeten worden binnen IT-outsourcing?

Om onderzoeksvraag 8 te beantwoorden is een nieuwe query gemaakt omdat nu een antwoord verkregen moest worden op de vraag of er ook gestuurd wordt met vertrouwen. Dit is de volgende query geworden:

1.) allintitle: trust (AND) risk (AND) control.

Deze query leverde 105 hits op.

Vervolgens is er gekeken naar het verband tussen trust en outsourcing middels de volgende query:

2.) allintitle: trust (AND) outsourcing

Deze query leverde 177 hits op.

Query aangescherpt met control, omdat de onderzoeksvraag het bewust sturen op trust bevat. Dat leverde de volgende query op:

2.a) allintitle: control (AND) trust (AND) outsourcing

Deze query leverde 21 hits op, waarbij de artikelen van Langfield –Smith en Heiskanen naar voren komen.

Vervolgens is de query aangescherpt met relationships, omdat het artikel van langfield-Smith spreekt over relationships. Dat leverde de volgende query op:

2.b) allintitle: trust (AND) relationships (AND) outsourcing

Deze query leverde 52 hits op.

Om onderzoeksvraag 8 te beantwoorden zijn met de bovenstaande query's in totaal 178 artikelen bekeken.

De eerste query leverde op:	105 artikelen
De tweede leverde op:	178 artikelen
Echter deze is aangescherpt door query 2a, die leverde op:	21 artikelen
En een tweede aanscherping, query 2b die leverde op:	<u>52 artikelen</u>
Dit is een totaal van:	178 artikelen

De bovenstaande resultaten van de query's zijn door de onderzoeker beoordeeld op titel en scannen van de inhoud van het artikel. Deze query's leverden ook resultaten op voor onderzoeksvraag 2.

3.2 Overzicht gebruikte literatuur

In de literatuurstudie zijn in totaal 27 artikelen gebruikt. Voorgaand aan het onderzoek is gekozen om maximaal 25 artikelen te gebruiken om de studielast te beperken. Echter in dit literatuuronderzoek zijn 27 artikelen gebruikt, omdat dit tot een completer onderzoek heeft geleid. Tijdens de selectie van deze artikelen is gekeken naar de meest relevant lijkende artikelen op basis

van het onderwerp, de context en het aantal citaties naar het gevonden artikel. Het is niet uit te sluiten dat er niet andere en wellicht meer passende artikelen zijn binnen de huidige literatuur.

Aan de hand van de query's zoals benoemd in 3.1 is een definitieve literatuurlijst opgesteld waarmee de antwoorden op de onderzoeksvraag en de deel onderzoeksvragen zijn gegeven.

In bijlage 2 is een overzicht van de tijdsvakken van verschijnen van de artikelen opgenomen, een overzicht van het aantal keren dat de gebruikte artikelen geciteerd is en het aantal artikelen per tertiaire bron.

3.3 Relevantie van de artikelen

De relevantie van de gevonden artikelen is beoordeeld aan de hand van het feit of deze antwoord geven op de opgestelde onderzoeksvragen. Hiervoor zijn criteria vastgesteld om de gevonden artikelen te beoordelen (Saunders M., 2015).

Voor dit onderzoek is bij de selectie van de artikelen rekening gehouden met de onderstaande criteria.

Bij het zoeken van de literatuur is niet ingeperkt op datum publicatie echter bij de beoordeling en de selectie van de gevonden artikelen is gekeken of deze artikelen na of in het jaar 1995 zijn geschreven. Deze keuze is gemaakt om er voor te zorgen dat de gevonden artikelen nog relevant zijn en de kans minder groot is dat het artikel is achterhaald.

Bij de artikelen die geselecteerd zijn is er gekeken naar de vraag: " Komt de context overheen met de onderzoeksvragen?"

Aantal keer dat er naar het artikel is gerefereerd.

4. Resultaten

Hieronder worden de resultaten vanuit het literatuuronderzoek weergegeven. Deze zijn per deelvraag uitgewerkt in een achttal subhoofdstukken:

Hoofdstuk 4.1 geeft antwoord op de vraag: "Wat wordt verstaan onder vertrouwen?"

Hoofdstuk 4.2 geeft antwoord op de vraag: " Welke relaties bestaan er tussen organisaties?"

Hoofdstuk 4.3 geeft antwoord op de vraag: " Wat wordt verstaan onder risicomanagement?"

Hoofdstuk 4.4 geeft antwoord op de vraag: "Wat zijn de risico's bij het outsourcen van IT?"

Hoofdstuk 4.5 geeft antwoord op de vraag: " Welke rol speelt vertrouwen bij vastlegging van afspraken tussen partijen?"

Hoofdstuk 4.6 geeft antwoord op de vraag: "Welke indicatoren van vertrouwen bestaan er vanuit de literatuur?",

Hoofdstuk 4.7 geeft antwoord op de vraag: " Is er een verband tussen risicomanagement en vertrouwen?"

Hoofdstuk 4.8 geeft antwoord op de vraag: " Op welke manier kan vertrouwen ingezet worden en hoe kan dit gemeten worden binnen IT-outsourcing?"

Hoofdstuk 4.9 bevat een verband tussen ITO risico's en trust: " Risico's van IT-Outsourcing die verband houden met Trustworthiness

Bij de uitwerking van het literatuuronderzoek staan twee vragen centraal:

Wat is er in de literatuur bekend over het onderwerp?

Wat is van belang in het onderzoek?

4.1 Wat wordt verstaan onder vertrouwen?

4.1.1 Wat is de definitie van vertrouwen

In de literatuur zijn vele definities van vertrouwen te vinden. In dit onderzoek wordt onderstaande definitie van Mayer (1995) gehanteerd, aangezien naar deze definitie in vele onderzoeken wordt verwezen en breed wordt gedragen binnen de literatuur (Rousseau, Sitkin, Burt, & Camerer, 1998).

“Vertrouwen is een psychologische toestand die de kwetsbaarheid accepteert op basis van positieve verwachtingen van de intenties of het gedrag van een ander” (Mayer, 1995).

Tortoriello ontleedt deze definitie en stelt dat in deze definitie twee elementen zitten (Bill McEvily, 2011):

de bereidheid om kwetsbaar te zijn.

de verwachting van een gunstige behandeling door een andere partij

Volgens Mayer zit er in deze definitie van vertrouwen de bereidheid om risico's te nemen en is dit in deze definitie de belangrijkste factor (Mayer, 1995). Indien er geen risico's zijn om te accepteren ontstaat er ook niets om te vertrouwen.

4.1.2 Welke soorten vertrouwen bestaan er die van toepassing kunnen zijn op de onderzoeksvraag?

Het consensusmodel van Earle (2010) stelt dat er twee vormen van vertrouwen zijn:

Het relationele vertrouwen (trust), dat is gebaseerd op de relatie tussen personen / organisaties. Dit vertrouwen is breed gedragen, veerkrachtig en vooral bezig met intenties.

Het berekenend vertrouwen (confidence), dat is gebaseerd op gedrag uit het verleden en op beperkingen op het gedrag van de toekomst. Dit vertrouwen is vooral gebaseerd op specifiek gedrag en is kwetsbaar.

Das en Teng (2001) definiëren vertrouwen als het hebben van twee dimensies, goodwill vertrouwen en competentie vertrouwen (Das, 2001). Competentie vertrouwen verwijst naar het **vermogen** van een partner om op basis van afspraken het werk uit te voeren en goodwill vertrouwen verwijst naar de **intentie** om dit te doen (Heiskanen, 2008).

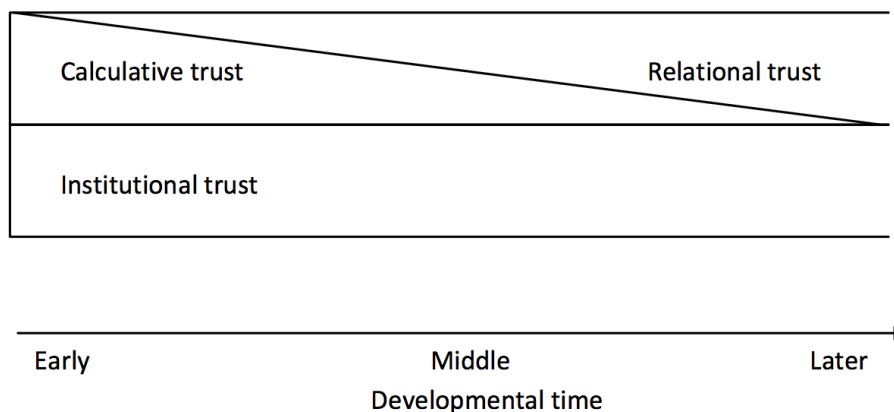
Rousseau onderscheidt verschillende vormen van vertrouwen. Net als Earle onderscheidt Rousseau het:

Calculatief of berekenend vertrouwen, dit is het vertrouwen dat is gebaseerd op rationele keuzes gerelateerd aan economische uitwisseling. Vertrouwen ontstaat wanneer de trustor waarneemt dat de trustee de neiging om een actie die gunstig is uit te voeren. Deze vorm van vertrouwen wordt beïnvloed door certificeringen en/of reputatie.

Relationele vertrouwen, dit is het vertrouwen dat zich gaandeweg ontwikkelt door herhaalde interacties tussen partijen.

Naast deze twee vormen onderscheid Rousseau ook het institutioneel vertrouwen. Deze relateert aan het vertrouwen dat instituten opwekken.

Het “Model of Trust” van Rousseau laat zien dat deze drie vormen van vertrouwen in elkaar over kunnen gaan, waarbij het institutioneel vertrouwen als een rode draad langs het berekende en relationele vertrouwen loopt.



Figuur 1: A model of trust (Rousseau et al.,1998)

4.1.3 Hoe kun je vertrouwen beïnvloeden?

Twee heuristieken die van belang zouden kunnen zijn in het beïnvloeden van vertrouwen zijn de *gelijkenis* heuristiek en de *invloed* heuristiek (Earle, 2010).

Gelijkenis heuristiek

Uit onderzoek (Al-Natour S, 2008) blijkt dat gelijkheid tussen personen, het spiegelen aan de ander, het vertrouwen verhoogt.

In het artikel van Timothy C. Earle worden twee gelijkenissen benoemd (Earle, 2010):

Gelijkheid van intenties, als de ander dezelfde intenties heeft dan wordt deze meer betrouwbaar geschat dan iemand die niet dezelfde intenties heeft.

Gelijkheid van waarden, volgens verschillende onderzoeken is er een sterk verband tussen waarde gelijkheid en betrouwbaarheid.

Invloed heuristiek

Invloed en vertrouwen zijn aan elkaar verbonden stelt Earle in zijn artikel. Als iemand invloed heeft op de ander of diens gedragingen zal het vertrouwen hoger zijn dan als die persoon geen invloed heeft op de ander of de gedragingen van de ander (Earle, 2010).

Hierin is “Trust” meer intern en toekomst gericht en minder afhankelijk van de invloed heuristiek en “Confidence” is meer extern en op het verleden gericht.

Hoewel houding en bepalingen vaak worden gezien als de belangrijkste onderlaag van het vertrouwen in de psychologie, volgens Inkpen (Inkpen, 2011) is het de actie die de trustor er toe brengt om te investeren in een relatie dat feitelijk het vertrouwen aantoont tussen twee actoren.

4.1.4 Samenvatting

In dit hoofdstuk is de breed gedragen definitie van vertrouwen uiteengezet welke door Mayer (1995) is opgesteld:

"Vertrouwen is een psychologische toestand die de kwetsbaarheid accepteert op basis van positieve verwachtingen van de intenties of het gedrag van een ander."

Er worden door Mayer twee typen vertrouwen benoemd: calculatief en relationeel vertrouwen, die tevens door meerdere auteurs gehanteerd worden. Omdat deze twee typen door meerdere onderzoeken gehanteerd worden is dit ook de definitie voor dit onderzoek.

Daarnaast zijn er twee heuristieken uiteen gezet, waarmee vertrouwen beïnvloed kan worden. In het kader van de onderzoeksvraag is het belangrijk om te weten welke soorten vertrouwen er zijn en met welk soort vertrouwen er gestuurd kan worden.

Elke relatie begint volgens (Rousseau et al., 1998) met calculatief vertrouwen, wat daarna langzaam overgaat in relationeel vertrouwen.

De gelijkenis heuristiek van Earle (2010) is voornamelijk van toepassing op het calculatief vertrouwen en de invloed heuristiek is meer gericht op het relationeel vertrouwen.

Aan de hand van de behandelde heuristieken kan een leverende partij een klant binnen halen en laten binden door het vertrouwen op deze manier te beïnvloeden. Hiermee kan er invloed uit geoefend worden te op het risicomanagement van de klant. De leverancier kan zijn gedrag, normen en waarden spiegelen aan de klant om zo te zorgen dat verwachtingen op elkaar aansluiten en dat potentiële klanten voor deze leverancier zullen kiezen.

4.2 Welke relaties bestaan er tussen organisaties?

4.2.1 Is het vertrouwen tussen organisaties anders dan tussen individuen?

Tomkins redeneert dat een organisatie gezien kan worden als een verzameling van personen die als een groep functioneren. Vervolgens geeft hij aan dat een groep vervolgens kan besluiten om vertrouwen te hebben in specifieke dingen, mensen of andere groepen. Tomkins concludeert derhalve dat, het zij het met aanpassingen, de proposities gerelateerd aan interpersoonlijk vertrouwen ook opgaan voor vertrouwen tussen organisaties (Tomkins, 2001).

4.2.2 Hoe ontwikkelt de relatie tussen leverancier en klant (of organisaties)?

Tomkins stelt dat naar mate de relatie volwassener wordt vanuit een start van lage mate van vertrouwen, er een positief verband is tussen vertrouwen en informatie. Dit komt omdat simpelweg vertrouwen zelf niet kan worden verhoogd zonder nadere informatie. Dus naar mate er meer informatie wordt uitgewisseld tussen partijen in het begin van de relatie, ontstaat er meer vertrouwen en zal er op den duur minder behoefte zijn aan meer informatie omdat het vertrouwen hoog is., dus omdat de mate van vertrouwen in latere stadia van de relatie hoger is, is het waarschijnlijk dat er minder informatie nodig is om die relatie behouden (Tomkins, 2001).

Indien tussen partijen herhaalde interactie plaats vindt, kan met succes een nauwere relatie ontstaan met een toenemende mate van vertrouwen tussen deze partijen. Het risico kan hierdoor beperkt worden, omdat de relatie niet snel zal instorten en de behoefte aan informatie om in

“controle te zijn” in de tijd minder zal worden. Hierdoor zal, in tegenstelling tot aan het begin van de relatie, waar veel informatie nodig is omdat er weinig vertrouwen is, er een inverse associatie plaats vinden tussen het verband van vertrouwen en gegevens. De groei wordt minder sterk, echter is er nog wel groei, maar als dit in een grafiek wordt weergegeven dan is deze groei als klokvorm weergegeven. Echter, in een vroeg stadium van een relatie, zijn toezeggingen meestal minder uitgebreid en zijn de risico's verbonden aan schending van deze verbintenis lager dan in latere stadia van de relatie (Tomkins, 2001).

4.2.3 Samenvatting

Voor dit onderzoek wordt de stelling van Tomkins (2001) aangenomen dat organisaties gezien kunnen worden als een verzameling personen die als een groep functioneren en derhalve de proposities van interpersoonlijk vertrouwen ook opgaat voor organisaties.

In dit hoofdstuk is tevens ingegaan op welke rol vertrouwen heeft binnen de relatie tussen organisaties, daarbij is het voor het onderzoek van belang waar in het proces deze rol zich bevindt in de relatie tussen organisaties. Daarbij is de invloed van vertrouwen in het begin van een relatie anders als bij een relatie die al verder gevorderd is. Daarbij kan met herhaalde interactie het risico reduceren omdat door deze interactie het vertrouwen tussen partijen hoger is.

Binnen de zoekcriteria zijn er meerdere artikelen naar voren gekomen die relaties tussen organisaties hebben benoemd echter is het artikel van Tomkins (2001) het enige artikel wat aansloot op dit onderzoek.

4.3 Wat wordt verstaan onder risicomanagement?

4.3.1 Wat is de definitie van risicomanagement?

De standaard van risicomanagement, ISO 31000, definieert risico management als:

Gecoördineerde activiteiten om het risico van de organisatie te sturen en controleren, gedefinieerd als een combinatie van de gevolgen van een gebeurtenis en de bijbehorende kans. Het risico management proces wordt gedefinieerd als de systematische toepassing van het management beleid, de procedures, activiteiten m.b.t. het communiceren, raadplegen, vaststellen van de context, en het identificeren, analyseren, evalueren, behandeling, monitoring, en reviewen van het risico (ISO Guide 73:2009, definitie 2.1).

Definitie van risico

In de definitie van risicomanagement zit tevens de definitie van risico:

Risico is het effect van onzekerheid op het behalen van doelstellingen.

Bij deze definitie van risico geeft het referentiekader ISO31000 een aantal opmerkingen:

Opmerking 1:

Een effect is een afwijking van de verwachting - positief en/of negatief;

Opmerking 2:

Doelstellingen kunnen worden gekenmerkt door verschillende aspecten (bijvoorbeeld financiële, arbo- of milieudoelen) en kunnen betrekking hebben op verschillende niveaus (zoals strategisch, organisatiebreed, een project, product of proces);

Opmerking 3:

Een risico wordt vaak gekarakteriseerd door verwijzing naar mogelijke gebeurtenissen en gevolgen

of een combinatie daarvan;

Opmerking 4:

Risico wordt vaak uitgedrukt als een combinatie van de gevolgen van een gebeurtenis (met inbegrip van wijzigingen in omstandigheden) en de bijbehorende waarschijnlijkheid dat de gebeurtenis zich voordoet;

Opmerking 5:

Onzekerheid is het geheel of gedeeltelijk ontbreken van informatie over, inzicht in of kennis van een gebeurtenis, de gevolgen daarvan, of de waarschijnlijkheid dat deze zich voordoet.

4.3.2 Welke soorten risico's zijn er te onderscheiden en welke is van toepassing op de onderzoeksvraag?

Aung (2008) heeft een classificatie gemaakt van operationele risico's bij IT-outsourcing, deze verdeelt hij in drie typen (Aung, 2008):

Externe risico's

Gedrags risico's

Proces risico's

Deze risico's staan hieronder in Tabel 2 opgenomen.

Tabel 2: *Classification of operational risk by risk event type*

	Event Type	Examples
External Risks	Damage to physical assets	Terrorism, vandalism, earthquakes, fires, and floods
	External fraud	Regional security breaches, Competitor's exploitation of trade secret at outsource provider's site
	Location related and business environment	Country risk, political risk, currency risk, visa restriction, travel restriction, Systemic vulnerability (external), pandemic risk, unexpected changes in competitive environment, service provider's business changes (M&A, Structure, Strategy, etc.)
Conduct Risks	Clients, products and business practices	Noncompliance to law, policies or ethical standards of service buyer, Misuse of trust, Misuse of customer information, Sale of unauthorized products, Vendor's exploitation of client's expertise
	Internal fraud	Data leakage, Employee theft, intentional misreporting, illegal trading of trade secret, IP
	Employment practices and workplace safety	Aviation Accidents, Personnel Security, Workers' compensation and discrimination claims, Violation of employee health and safety rules, and general liability
Process Risks	Business disruption and system failures	Provider's bankruptcy, Security & system vulnerability (increase in security holes), Systemic Vulnerability (internal),

		HW/SW failures, telecommunication problems and utility outages
	Execution, delivery, and process management	SLA management, Service debasement (failure in process and quality control), Exception handling, Seasonality handling, non-standardized measurement, Miscommunication, vendor dispute, inaccuracy in reporting, incomplete legal documentation

(Aung, 2008)

Binnen dit onderzoek zijn de gedragsrisico's voornamelijk van belang. Vertrouwen is een "zachte" factor en valt onder gedrag. De onderzoeksvraag is er op gericht om te onderzoeken of de gedragsrisico's te verminderen zijn aan de hand van vertrouwen met betrekking tot klanten, producten en bedrijfsactiviteiten.

Risicomanagement zou ook hierop kunnen reageren, maar dit valt buiten de scope van dit onderzoek.

Volgens Stolen (Mass Soldal Lund, 2010) is vertrouwen inherent gerelateerd aan risico. Een belangrijk deel van het managen van risico's is het begrijpen van de risico's die met Trust interactie te maken hebben. Stolen stelt dat trust een overtuiging is die de trustor heeft ten opzichte van de trustee met betrekking tot een bepaalde handeling waarbij de mate variërend tussen 0 (geen vertrouwen) en 1 (volledig vertrouwen).

Idealiter, zijn vertrouwen en controle in evenwicht op een zodanige wijze dat zowel de klant en de leverancier ervan overtuigd zijn dat de relatie gunstig is en dat zij bereid zijn om het voort te zetten en tevreden met de resultaten zullen zijn. Volgens de literatuur zijn vertrouwen en controle ingewikkelde begrippen (bijvoorbeeld: (Inkpen, 2011); (Nooteboom, 2000; Rosalinde Klein Woolthuis, 2005) (Das en Teng, 1998, 2001)).

4.3.3 Samenvatting

De verzameling van Aung is een classificatie van operationele risico's die plaats kunnen vinden bij IT-Outsourcing. Deze classificatie is nodig voor dit onderzoek om de ITO (IT-Outsourcing) risico's te classificeren. Aan de hand van onder andere deze classificatie kan vastgesteld worden over deze ITO risico's verband hebben met vertrouwen.

4.4 Wat zijn de risico's bij het outsourcen van IT?

4.4.1 Wat wordt verstaan onder outsourcen van IT?

Een definitie van outsourcing is: Het uitbesteden van een dienst of activiteit aan een derde partij (Langfield-Smith, 2001).

Het uitbesteden van diensten en / of producten wordt ook steeds vaker toegepast in de Informatie Technologie. Hier wordt het Information Technologie Outsourcing (ITO) genoemd, wat er op neer komt dat alle IT-bezittingen, resources en activiteiten worden overgedragen aan een derde partij die dit gaat beheren.

Sinds eind van de jaren 80 is het concept ITO gegroeid tot een strategische management keuze.

4.4.2 Wat zijn de voor en nadelen van IT-outsourcing?

De voordelen van ITO kunnen worden ondergebracht in drie categorieën (Urbach & Wurz, 2012):

- strategische voordelen;
- economische voordelen;
- technologische voordelen.

Kadabadse (2000) onderscheidt voor- en nadelen van outsourcing. De voordelen die benoemt worden zijn:

- het bestaande personeel kan zich concentreren op de kernactiviteiten van de organisatie, met de nadruk op het bereiken van de belangrijkste strategische doelstellingen, (Als strategisch voordeel benoemd door Urbach & Wurz (2012))
- het verminderen of stabiliseren van overhead kosten, en daarmee kostenvoordeel verkrijgen ten opzichte van de concurrentie (Als economisch voordeel benoemd door Urbach & Wurz (2012))
- het verminderen van de investeringen in technologie (Als technologisch voordeel benoemd door Urbach & Wurz (2012))

De nadelen die Kadabadse benoemt zijn:

- afhankelijkheid van externe leveranciers
- niet de vermeende kostenbesparingen realiseren
- de controle verliezen op kritieke functies
- outsourcing kan nieuwe risico's met zich meebrengen, zoals het verlies van kritische vaardigheden of het ontwikkelen van de verkeerde vaardigheden,
- het verlies van de cross-functionele vaardigheden
- het verlies van controle over de leveranciers

(Kadabadse, 2000)

4.4.3 Wat zijn de risico's van IT-outsourcing?

Er gaat normaal gesproken een heel proces aan vooraf voordat er gekozen wordt voor een partij die voldoet aan de eisen. Hierbij hoort vaak ook een risicoanalyse, waarbij naast de risico's ook de voor en nadelen worden beschreven van het outsourcen van de IT.

Belangrijk is het voor een organisatie om een juiste keuze te maken voor een leverancier, want het is voor organisaties lastig om te switchen van leverancier indien ze eenmaal gekozen hebben voor een leverancier waar zij hun ICT aan uitbesteden. Het hele proces van overdracht en keuze hebben dan al zo veel gekost dat een weg terug niet meer reëel is. Hierdoor is typerend voor het outsourcen van informatiesystemen dat het heel kostbaar is voor de klant om van leverancier te wisselen (Heiskanen, 2008).

Naast objectieve indicatoren bestaan er ook wat "zachtere" indicatoren waarop gestuurd zou kunnen worden tijdens de risico analyse.

J. Tetteroo heeft in zijn literatuuronderzoek een overzicht gemaakt waarbij hij alle ITO risico's, die hij heeft gevonden in de literatuur, heeft opgenomen. Daarbij heeft hij verschillende risico's gecombineerd, omdat deze 1 of meerdere overeenkomsten bevatten. Het overzicht dat is overgebleven betreft 38 ITO risico's, deze is in bijlage 3 opgenomen (Tetteroo, 2016).

4.4.4 Samenvatting

In dit hoofdstuk is aangegeven wat er verstaan wordt onder IT-outsourcing, wat de voor en nadelen zijn en wat de risico's zijn bij IT-outsourcing. Hiervan is een duidelijk beeld ontstaan voor de onderzoeksvraag. Welke risico's van IT-outsourcing moeten gereduceerd worden en waar vallen deze onder als er gesproken wordt over vertrouwen.

Om inzicht te verkrijgen van de voordelen en nadelen van ITO risico's is van belang zodat er gekeken kan worden welke voordelen te behalen zijn als er bewust gestuurd kan worden op factoren van vertrouwen bij ITO risico's. Zo zijn deze voor en nadelen onderverdeeld in strategische, economische en technologische voordelen (Urbach & Wurz, 2012).

Als de perceptie van de ITO risico's lager wordt ingeschat, zullen er minder maatregelen nodig zijn om dit risico af te dekken, dan wanneer deze perceptie van dit risico hoger wordt ingeschat

4.5 Welke rol speelt vertrouwen bij vastlegging van afspraken tussen partijen?

4.5.1 Op welke manieren worden afspraken vastgelegd tussen organisaties

Afspraken kunnen vastgelegd worden in Service Level Agreements (SLA's), Dossier Afspraken en Procedures (DAP) etc., maar het is niet mogelijk om elke onvoorziene gebeurtenis in een gesloten overeenkomst te specificeren gedurende een lange periode (Heiskanen, 2008).

Vertrouwen speelt namelijk een belangrijke rol tussen samenwerkingsverbanden. Bij samenwerkingsrelaties bestaan er grofweg drie vormen regels c.q. afspraken waar de organisaties mee te maken krijgen (Kavan, 2005):

De formele processen moeten bij een samenwerkingsrelaties opnieuw vorm krijgen en worden ingericht en bestuurd.

Contracten met afspraken m.b.t. de samenwerking zullen worden opgesteld.

Informele processen. Vertrouwen is bijvoorbeeld een belangrijke succesfactor voor samenwerkingsrelaties en wordt door velen gezien als een noodzakelijke factor om onzekerheden, c.q. risico's te overbruggen.

Onderzoek naar governance van IT outsourcing heeft geleid tot het herkennen van twee momenten van governance: het formele outsourcing contract (promissory contract) en het post-contractuele relatie management (psychologisch contract). (Rousseau, 2001; Rousseau et al., 1998) (Kavan, 2005)

Een formele overeenkomst tussen de partijen zou kunnen uitgroeien tot een relationele overeenkomst (Heiskanen, 2008). Deze relationele overeenkomst die Heiskanen benoemt komt overeen met het psychologisch contract van Rousseau. De invloed die partijen kunnen uitoefenen vormt de basis van de manier waarop de relatie wordt beheerd tijdens lange contractuele perioden. Power, vertrouwen en controle zijn belangrijke begrippen hier.

Een psychologisch contract refereert naar een individueel psychisch geloof met betrekking tot zijn of haar gelijke verplichtingen in een contractuele relatie (Rousseau, 2001).

De psychologisch contract theorie biedt een zeer relevante en solide theoretische lens voor het bestuderen van IT-outsourcing management omwille van zijn drie verschillende principes (Rousseau, 2001):

- de focus op wederzijdse (in plaats van eenzijdig) verplichtingen tussen de contractuele partijen
- de nadruk op de psychologische (in tegenstelling tot wettelijke) verplichtingen
- de nadruk op individuele (in plaats van inter-organisatorische) niveau van analyse

Het eerste principe in het psychologische contract is de erkenning van de wederkerigheid bij de contractuele relatiepartijen . Wederkerigheid is verankerd in de wederzijdse relatie tussen de twee partijen. Wederzijdse verplichtingen leiden tot een geloof in wat men verplicht is om op basis van gepercipieerde beloften van een onderlinge uitwisseling te bieden . Het concept van wederkerigheid benadrukt dus het belang van het kijken naar gepercipieerde verplichtingen vanuit het perspectief dat beide partijen betrokken zijn, in plaats van slechts één perspectief . Een psychologisch contract bestaat alleen als beide partijen van mening zijn dat een overeenkomst bestaat, dat de gemaakte afspraken zijn gemaakt en die overwegingen in ruil zijn aangeboden(Rousseau, 2001) .

Wederkerigheid betekent in wezen " dat de partijen die betrokken zijn in feite te houden zijn aan dezelfde opvattingen ten aanzien van hun verplichtingen jegens elkaar " (Koh, 2004; Rousseau, 2001).

Het psychologisch contract staat dus los van het formele contract, dat een contract is dat verbonden is aan regels en onderworpen aan derden interpretaties (zoals bijvoorbeeld het rechtssysteem). Dit onderscheid is belangrijk omdat , ongeacht of een formele overeenkomst bestaat, individuen psychologische contracten ontwikkelen. Uiteindelijk is het de individuele overtuigingen en percepties van deze verplichtingen (dat wil zeggen, het psychologisch contract), in plaats van het werkelijke schriftelijk contract, dat het gedrag stuurt . Het psychologisch contract omvat percepties en overtuigingen van zowel uitdrukkelijke schriftelijke termen in het juridische contract en impliciete ongeschreven termen van de partijen (Koh, 2004).

Koh poneert dat succesvolle IT-outsourcing sterk afhankelijk is van een psychologisch contract tussen de klant en de leverancier. Deze psychologische contractverplichtingen kunnen worden geschreven in de voorwaarden van een juridisch contract , of gewoon gebaseerd op mondelinge toezeggingen en andere uitingen van de toezegging van de partijen (Koh, 2004).

Het psychologisch contract is een constructie op individueel niveau en het is daarom af te vragen of het van toepassing kan zijn op een fenomeen op organisatorisch niveau, zoals IT-outsourcing . Zoals Rousseau namelijk vurig betoogt , " individuen hebben psychologische contracten , organisaties niet" (Rousseau 1989)(Koh, 2004) .

Toch is Koh et al. (Koh, 2004) van mening dat het concept van een psychologisch contract zeer relevant is voor de context van IT- outsourcing. In feite laten we zien dat door te focussen op het individuele niveau van de analyse van het gebruik van psychologische contracten dat dit zorgt voor een unieke en tot nu toe weinig bestudeerd perspectief op de outsourcing relaties die ontstaan tussen organisaties (Koh, 2004).

4.5.2 Is er een verband tussen het vastleggen van afspraken en vertrouwen tussen partijen?

Klein Woolthuis (2005) stelt dat drie verschillende opvattingen heersen over de rol van contracten en hun invloed op vertrouwen.

het contract als basis voor vertrouwen, omdat het de mogelijkheden en de prikkels voor opportunisme (snel voordeel) beperkt. Hierdoor kunnen partijen elkaar vertrouwen, omdat ze geen andere optie hebben dan om zich betrouwbaar op te stellen. (hun opportunisme zal ten koste gaan van de sancties). Hier zijn het contract en vertrouwen positief gerelateerd, met een contract als voorwaarde voor vertrouwen.

contracten kunnen schadelijk zijn voor de ontwikkeling van vertrouwen, omdat de contracten kunnen worden geïnterpreteerd als een teken van wantrouwen. Ook kan actief gebruik van het contract (bijvoorbeeld door monitoring, bedreiging of rechtszaken), het conflict, opportunisme en defensief gedrag oproepen.

De derde interpretatie van de relatie tussen vertrouwen en contract stelt dat vertrouwen en het contract een negatief verband hebben. Als vertrouwen al bestaat voorafgaand aan de 'inbedding' van de relatie, zal er minder behoefte zijn aan formele controle of contracten. In deze visie, als vertrouwen voorafgaat aan de relatie zullen contracten als gevolg overbodig worden.

Er is een fundamentele onenigheid in de literatuur over de relatie tussen vertrouwen en controle en de vraag hoe vertrouwen en het contract gerelateerd zijn (Rosalinde Klein Woolthuis, 2005).

Uit het onderzoek van Klein Woolthuis (2005) komen de volgende conclusies naar voren:

dat vertrouwen in het algemeen zal voorafgaan aan het contract.

dat vertrouwen en contracten zowel substituten als complementen kunnen zijn van elkaar. Dit hangt af van de intenties waarmee contracten worden opgesteld en worden gebruikt. Ten eerste, als een contract niet wordt geïnterpreteerd als een strikt juridische bescherming, kunnen vertrouwen en een contract heel goed hand in hand gaan, in welk geval vertrouwen en contract complementair zal zijn. Ten tweede, als partijen elkaar vertrouwen, kunnen ze er voor kiezen om geen beschermende clausules in hun contract op te nemen, in welk geval het vertrouwen het contract vervangt. Ten derde, in situaties van hoog wantrouwen, kunnen partijen grote nadruk leggen op contracten en aan een gedetailleerde behoud van clausules, in welk geval het contract het gestelde vertrouwen vervangt.

dat relaties die gekenmerkt werden door vertrouwen meer succesvol waren. Dit ondersteunt eerdere claims van sociale wetenschappers dat vertrouwen een belangrijke voorwaarde is om een open en constructieve sfeer te creëren.

4.5.3 Samenvatting

Vanuit de literatuur is naar voren gekomen dat er een verband is tussen het vastleggen van afspraken in verschillende contracten, zowel formeel als psychologisch en het vertrouwen wat bestaat tussen organisaties.

In dit hoofdstuk is het onderscheid gemaakt tussen het formele contract en het psychologische contract. Uit de literatuur blijkt dat vertrouwen een onderdeel is van het psychologische contract. En sterk psychologisch contract is de basis voor een goede samenwerking en een geslaagde IT-outsourcing.

Alhoewel veel onenigheid is in de literatuur over de relatie tussen vertrouwen en controle, stelt Woolthuis (2005) dat er drie opvattingen heersen over contracten en hun invloed op vertrouwen. De belangrijkste conclusie uit het onderzoek van Woolthuis(2005) is dat de relaties waarbij er veel vertrouwen is, deze het meest succesvol waren in hun samenwerking.

Voor dit onderzoek is dit belangrijk om te weten, omdat hieruit blijkt dat de onderzoeksvraag relevant is, aangezien vertrouwen een belangrijke voorwaarde is om een succesvolle relatie aan te gaan of te hebben tussen partijen. Indien dit vertrouwen tussen relaties ook bewust beïnvloed kan worden om de perceptie van risico's te reduceren kan de relatie mogelijk nog succesvoller worden.

4.6 Welke indicatoren van vertrouwen bestaan er vanuit de literatuur?

4.6.1 Wat is er in de literatuur bekend over factoren van vertrouwen die een rol spelen bij outsourcen van IT

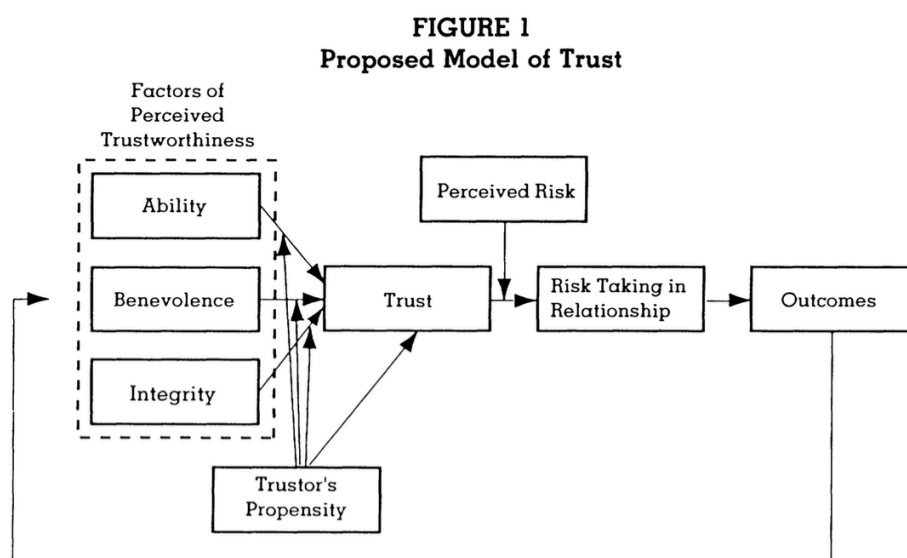
Voor het vertrouwen in IT outsourcing wordt een typische indeling gepresenteerd door Sabherwal (1999), die vier types van vertrouwen heeft gevonden (Heiskanen, 2008):

- Calculated trust
- Knowledge-based trust
- Identification-based trust
- Performance-based trust

Echter, deze classificaties van vertrouwen werden bekritiseerd door (Bachmann, 2001), die beweerde dat het twijfelachtig is of dergelijke concepten men helpt om meer vat te krijgen op het fenomeen vertrouwen zelf. Hij dringt erop aan dat er veel theoretische input nodig is om volledig te begrijpen hoe vertrouwen werkt als een governance-mechanisme binnen trans-organisatorische relaties. Het kritiek punt van Bachmann lijkt te zijn dat een meer inzichtelijke classificatie van vertrouwen is vereist (Heiskanen, 2008).

Veel onderzoekers zijn het eens met Deutsch (1958), dat het bestaan van risico of iets geïnvesteerd hebben, vereist is voor vertrouwen. De behoefte aan vertrouwen ontstaat slechts in een risicovolle situatie. Mayer stelt dat het onduidelijk is of risico een gedrags beïnvloedende factor is die aan het vertrouwen voorafgaat, of dat het risico het vertrouwen is of dat risico een resultaat is van vertrouwen (Mayer, 1995).

Mayer heeft een model ontwikkeld waarbij de concentratie ligt op het vertrouwen in een organisatorische setting waarbij twee specifieke partijen deelnemen: een vertrouwende partij (trustor) en een partij te vertrouwen (trustee).



Figuur 1: Model of Trust (Mayer, 1995)

In het model van Mayer wordt risico gescheiden van het vertrouwen. Vertrouwen brengt niet perse risico met zich mee, maar een bereidheid om een risicovolle relatie aan te gaan met de trustee (bijvoorbeeld: het delen van vertrouwelijke informatie) (Gill, 2005).

Dit model past daarmee perfect op de onderzoeksvraag. Als er meer trust (in Figuur 1) is, zal het 'perceived risk' lager zijn. De 'factors of perceived trustworthiness' zijn dus mogelijk belangrijke input- c.q. stuurfactoren voor het verlagen van het gepercipieerde risico.

4.6.2 Wat is de definitie van deze indicatoren

Mayer (1995) stelt in zijn artikel dat omstandigheden die leiden tot vertrouwen herhaaldelijk zijn onderzocht in de literatuur. Daar bij zegt Mayer dat er auteurs zijn die een enkele eigenschap identificeren die verantwoordelijk is voor vertrouwen (bijvoorbeeld, Strickland, 1958), terwijl andere auteurs er maar liefst 10 eigenschappen aan toe kennen (bijvoorbeeld Butler, 1991) (Mayer, 1995).

Mayer (1995) heeft naar aanleiding van een analyse op 23 artikelen een overzicht van de antecedenten van vertrouwen gepubliceerd tussen 1958 en 1993. Een overzicht van de factoren die leiden tot vertrouwen is door Mayer samengevat in Tabel 2.

Tabel 3: *Antecedenten van Trust (Mayer, 1995)*

Trust Antecedents	
Authors	Antecedent Factors
Boyle & Bonacich (1970)	Past interactions, index of caution based on prisoners' dilemma outcomes
Butler (1991)	Availability, competence, consistency, discreteness, fairness, integrity, loyalty, openness, promise fulfillment, receptivity
Cook & Wall (1980)	Trustworthy intentions, ability
Dasgupta (1988)	Credible threat of punishment, credibility of promises
Deutsch (1960)	Ability, intention to produce
Farris, Senner, & Butterfield (1973)	Openness, ownership of feelings, experimentation with new behavior, group norms
Frost, Stimpson, & Maughan (1978)	Dependence on trustee, altruism
Gabarro (1978)	Openness, previous outcomes
Giffin (1967)	Expertness, reliability as information source, intentions, dynamism, personal attraction, reputation
Good (1988)	Ability, intention, trustees' claims about how (they) will behave
Hart, Capps, Cangemi, & Caillouet (1986)	Openness/congruity, shared values, autonomy/feedback
Hovland, Janis, & Kelley (1953)	Expertise, motivation to lie
Johnson-George & Swap (1982)	Reliability
Jones, James, & Bruni (1975)	Ability, behavior is relevant to the individual's needs and desires
Kee & Knox (1970)	Competence, motives
Larzelere & Huston (1980)	Benevolence, honesty
Lieberman (1981)	Competence, integrity
Mishra (In press)	Competence, openness, caring, reliability
Ring & Van de Ven (1992)	Moral integrity, goodwill
Rosen & Jerdee (1977)	Judgment or competence, group goals
Sitkin & Roth (1993)	Ability, value congruence
Solomon (1960)	Benevolence
Strickland (1958)	Benevolence

Mayer categoriseert en definieert de 3 factoren die ook in het model of Trust benoemd zijn:

- Ability (bekwaamheid, kundigheid)
- Benevolence (welwillendheid)
- Integrity (integriteit)

Als set, lijken deze drie een groot deel van trustworthiness (betrouwbaarheid) te verklaren. Elk van deze drie draagt bij aan een uniek perspectief van vertrouwen, terwijl alle drie samen een solide en spaarzaam fundament biedt voor de empirische studie van vertrouwen voor een andere partij (Mayer, 1995).

McEvily stelt tevens dat vertrouwen een veelzijdige constructie is. Gezien de complexiteit, lijkt het in veel gevallen passend om vertrouwen te zien als een multidimensionale constructie en empirisch te evalueren in verschillende dimensies, waarbij het bestaan, de aard en de mate van hun relatie tot elkaar wordt onderzocht. De overgrote meerderheid van de onderzoeken naar vertrouwen behandelt vertrouwen als een 1- dimensionale constructie.

In bijlage 5 van dit rapport wordt een overzicht weergegeven van het onderzoek van McEvily, waarbij de dimensies van vertrouwen zijn weergegeven en het aantal keer dat het onderzocht is. McEvily telde een totaal van 38 verschillende dimensies van vertrouwen (Bill McEvily, 2011).

De drie factoren die Mayer in zijn model benoemt staan ook in deze lijst, en wel op nummer 1,2 en 3:

- Integrity
- Ability
- Benevolence

Ook Pytlikzillig (2016) stelt dat een van de meest geciteerde modellen van vertrouwen in de literatuur het Trustworthiness model van Mayer (1995) is met de drie dimensies: ability, benevolence, en integrity (Lisa M. PytlikZillig, 2016).

De relatie tussen de drie antecedenten (integrity, ability en benevolence) en vertrouwen wordt ondersteund door het onderzoek van Gill (Gill, 2005) en het onderzoek van Heyns (Heyns, 2015).

4.6.3 Samenvatting

Het model van Mayer (1995) wordt vaak aangehaald binnen de literatuur en breed gedragen door andere onderzoekers. In veel onderzoeken zie je de begrippen: Integrity, ability en benevolence, terugkomen. Hieruit kan opgemaakt worden dat dit de belangrijkste factoren zijn voor het meten van vertrouwen, samen met elkaar lijken deze drie een groot deel van trustworthiness te verklaren.

Echter, een kanttekening bij het meten van vertrouwen is dat er in de praktijk geen groot verschil is in metingen tussen vertrouwen en trustworthiness. In tegenstelling tot vertrouwen, verwijst trustworthiness naar overtuigingen, evaluaties, of verwachtingen van de doelgroep die volgens de theorie vaak de basis voor vertrouwen vormen. De verschillen tussen vertrouwen en trustworthiness worden vaak bestempeld als theoretisch belangrijk, tevens geven onderzoekers ook vaak aan dat vertrouwen of dimensies van vertrouwen bestuderen terwijl ze in werkelijkheid trustworthiness onderzoeken. Het verschil tussen vertrouwen en trustworthiness is vanuit theoretisch perspectief wel duidelijk, maar vertrouwen en trustworthiness zijn zeer nauw verwant. De metingen van vertrouwen en trustworthiness wordt in de praktijk vaak onduidelijk, zodat het meten van een van de factoren van de een ook steeds goede indicatoren van de andere zijn. Het is

dus niet zeker dat alle metingen van vertrouwen en trustworthiness statistisch verschillend zullen zijn (Lisa M. PytlikZillig, 2016).

Hiermee zou in het vervolgonderzoek rekening gehouden moeten worden.

4.7 Is er een verband tussen risicomanagement en vertrouwen?

4.7.1 Bestaan er onderzoeken naar de verbanden tussen risicomanagement en vertrouwen?

Drie belangrijke reviews van vertrouwen binnen risicomanagement die naar voren zijn gekomen binnen dit literatuuronderzoek:

Earle (2010), Trust in Risk Management: A Model-Based Review of Empirical Research (Earle, 2010).

Chryssochoidis G, Strada A, Krystallis A (2009). Public trust in institutions and informationsources regarding risk management and communication.: Towards integrating extant knowledge (Chryssochoidis G, 2009).

Lisa M. Pytlikzillig, Joseph A. Hamm, Ellie Shockley, Mitchel N. Herian, Tess M.S. Neal, Christopher D. Kimbrough, Alan J. Tomkins & Brian H. Bornstein, The dimensionality of trust-relevant constructs in four institutional domains: results from confirmatory factor analyses (Lisa M. PytlikZillig, 2016).

Het artikel van Earle is een review artikel die is opgesteld om de relatie te onderzoeken tussen verschillende onderzoeken naar trust en het consensus model of trust. Het consensus model specificert twee conceptualisaties van vertrouwen, het relationeel en het berekenend vertrouwen. Uit de resultaten van dit onderzoek bleek dat de meeste studies van trust in risicomanagement, voor een deel overeen kwamen met het consensus model. De evaluatie concludeert dat er aangedrongen moet worden op een betere integratie tussen beide conceptualisaties.

Het artikel van Chryssochoidis probeert een review te geven van de kennis over het publieke vertrouwen binnen instellingen en over de informatiebronnen met betrekking tot risicobeheer en communicatie. Deze review is gebaseerd op 27 empirische studies en is georganiseerd rond vier groepen die een samenhang hebben met vertrouwen. Chryssochoidis et al heeft er voor gekozen om geen theoretisch model te ontwikkelen maar om patronen te beschrijven die voortgekomen zijn uit de beschrijvingen van verschillende empirische studies.

Pytlikzillig heeft onderzoek gedaan naar een groot aantal studies die vertrouwen constructies hebben onderzocht, verdeeld over vier institutionele contexten (politie, lokaal bestuur, natuurlijke hulpbronnen, staatsbestuur). In de verschillende studies zijn een aantal gemeenschappelijke bevindingen naar voren gekomen.

Pytlikzillig (2016) stelt dat een van de meest geciteerde modellen van vertrouwen in de literatuur het Trustworthiness model van Mayer (1995) is.

Deze review artikelen bevestigen de keuze van de literatuur zoals deze is gekozen door de onderzoeker en gebruikt in dit literatuuronderzoek. Uit deze artikelen komt naar voren dat het consensus model van Earle en het trustworthiness model van Mayer, twee belangrijke modellen zijn met betrekking tot trust.

4.8 Op welke manier kan vertrouwen ingezet worden en hoe kan dit gemeten worden binnen IT-outsourcing?

4.8.1 Zijn er modellen om onderzoek te doen naar vertrouwen binnen risicomanagement?

In het artikel van Earle (2010), *Trust in Risk Management: A Model-Based Review of Empirical Research*, heeft Earle verschillende modellen uiteengezet waarbij vertrouwen een rol speelt binnen het risicomanagement. Deze modellen zijn hieronder benoemd en verder toegelicht in bijlage 5:

- Consensusmodel
- TCC Model
- The Associationist model
- The integrative model
- Consumer Confidence model (CCM)
- Social Trust, Epistemic Trust, and Antagonism

De modellen van vertrouwen in risicomanagement, die Earle (2010) benoemt in zijn artikel, geven aan dat, alhoewel verschillende modellen beschikbare alternatieven geven voor de elementen van het consensus model, geen van de modellen fundamentele meningsverschillen hebben met het consensus model. Het komt er op neer dat alle modellen in meer of mindere mate de elementen, relationeel vertrouwen en calculatief vertrouwen, van het consensusmodel gebruiken.

4.8.2 Zijn er modellen waarmee het vertrouwen gemeten kan worden?

Om vertrouwen te meten zijn er tevens verschillende modellen ontwikkeld. Deze zijn door McEvily uiteengezet (Bill McEvily, 2011).

McEvily stelt in zijn review dat er een toenemende behoefte is om vertrouwen te operationaliseren, oftewel te meten. Binnen de organisatie literatuur wordt er steeds meer geschreven en onderzocht m.b.t. vertrouwen binnen en tussen organisaties. Hoe dit vertrouwen geoperationaliseerd wordt, is minder duidelijk en zijn er veel minder onderzoek en modellen die laten zien hoe (factoren van) vertrouwen gemeten kan worden.

McEvily heeft de onderzoeken die hier onderzoek naar hebben gedaan onderzocht in deze review en heeft de onderzoeken die gerepliceerd en gevalideerd zijn eruit gelicht.

In chronologische volgorde zijn de vijf onderzoeken van het meten van vertrouwen, die gerepliceerd en gevalideerd zijn, die McEvily heeft onderzocht:

1. McAllister (1995), Managerial Interpersoonlijke Trust
2. Currall en Judge (1995), Trust Boundary Role Personen '
3. Cummings en Bromiley (1996), Organisational Trust Inventory
4. Mayer en Davis (1999) Organisational Trust
5. Gillespie (2003), Behavioural Trust Inventory

McEvily beschrijft, in het overzicht van bijlage 6, de onderscheidende kenmerken van elk van de onderzoeken.

4.8.3 Samenvatting Modellen

Uit de evaluatie van het artikel van Earle (2010) is gebleken dat de meeste studies van vertrouwen in risicomanagement tenminste gedeeltelijk overeen komen met de aanpak van de consensus model.

Vanuit dit literatuuronderzoek kwam al naar voren dat het model van Mayer als best geschikt was bevonden (zie 4.6), dit wordt door het onderzoek van McEvily bevestigd. Het model van Mayer is repliceerbaar en tevens gevalideerd.

Het model of trust van Mayer is gebaseerd op studies binnen het gebied van organisatie vertrouwen, een studie gebied die de neiging heeft om meer systematische en model-based te zijn dan studies van vertrouwen in risicomanagement.

Voor dit onderzoek is het model van Mayer belangrijk, omdat dit model gebruikt kan worden voor een vervolgonderzoek naar de onderzoeksvraag of er bewust gestuurd kan worden met factoren van vertrouwen binnen het risicomanagement.

Door het gebruik van beide modellen, Earle en Mayer, wil de onderzoeker beiden studiegebieden bij elkaar brengen: het model van Mayer gebaseerd op de drie factoren van trustworthiness (organisatie vertrouwen) en het consensus model van Earle (vertrouwen in risicomanagement).

Door deze twee gebieden bij elkaar te brengen kan een nieuw model ontstaan die vanuit beide modellen opgesteld kan worden. Een vervolgonderzoek zou kunnen zijn om dit model te gaan ontwikkelen.

4.9 Risico's van IT-Outsourcing die verband houden met Trustworthiness

In dit literatuuronderzoek is enerzijds een lijst met risico's van IT-Outsourcing benoemd welke is opgesteld door J. Tetteroo en anderzijds zijn factoren van trustworthiness, zoals Mayer deze heeft gedefinieerd in zijn model, benoemd.

Om een verband te leggen tussen de risico's van IT-outsourcing en trustworthiness heeft de onderzoeker, in dit literatuuronderzoek, getracht om deze bij elkaar te brengen.

Aan de hand van de gedefinieerde risico's van IT-outsourcing, zie de Tabel van J. Tetteroo bijlage 3, is door de onderzoeker geïnterpreteerd welke ITO risico's een verband hebben met vertrouwen. Daarbij is tevens gekeken naar welke factor van trustworthiness (integrity, benevolence, ability (Mayer, 1995)), dit risico beïnvloed, deze is in de vierde kolom van de Tabel 6 weergegeven.

De drie factoren die Mayer benoemd die te maken hebben met trustworthiness heeft de onderzoeker naast de risico's van IT-outsourcing gelegd. Hierdoor blijft een lijst over van ITO risico's die specifiek gericht zijn op de factoren van trustworthiness. Deze lijst is gebaseerd op de interpretatie van de onderzoeker, om de keuzes helder inzichtelijk te maken is deze interpretatie in bijlage 4 opgenomen.

Dit bij elkaar brengen van de IT-outsourcing risico's en de factoren van trustworthiness heeft geresulteerd in onderstaande Tabel 6, met 12 ITO risico's.

Deze 12, door de onderzoeker, geselecteerde ITO risico's die verband houden met vertrouwen zijn onder te verdelen in de gedrags risico's van Aung. Deze onderverdeling is gebaseerd op de interpretatie van de onderzoeker, om de keuzes helder inzichtelijk te maken is deze interpretatie in bijlage 4 opgenomen, de onderverdeling staat in de laatste kolom van Tabel 6.

De gedragsrisico's die Aung benoemd waren ingedeeld in drie groepen:

1. Cliënten, producten en business (Bijv. niet voldoen aan wetgeving, misbruik van vertrouwen, misbruik van informatie over klanten, verkoop van niet-toegestane producten)

2. Interne fraude (Bijv. lekken van gegevens, diefstal door medewerkers, opzettelijk onjuiste rapportage, illegale handel in handelsgeheimen, beter voordoen van de cijfers)

3. Werkgelegenheid en veiligheid op de werkplek (Bijv. ongevallen, personeels veiligheid, overtreding van de regels mbt gezondheid en veiligheid van werknemers en algemene aansprakelijkheid)

Tabel 4: ITO risico's met betrekking tot vertrouwen

#	ITO Risico's (Tetteroo, 2016)	Van toepassing op vertrouwen	Factor van vertrouwen	Gedrag risico's van Aung
1	Backlash from internal IT staff	X	Integrity	Werkgelegenheid en veiligheid op de werkplek
2	Contractual risk	X	Integrity, benevolence, ability	Cliënten, producten en business
3	Coordination between client and supplier	X	Integrity, benevolence, ability	Cliënten, producten en business
4	Cultural differences between client and supplier	X	Integrity, benevolence	Cliënten, producten en business
5	Difficulty in managing remote teams	X	Integrity, benevolence	Cliënten, producten en business
6	Lack of trust	X	Integrity, benevolence, ability	Cliënten, producten en business
7	Loss of control over data	X	Integrity, ability	Interne fraude
8	Opportunistic behaviour	X	Integrity, benevolence	Interne fraude
9	Security / privacy breach	X	Integrity	Interne fraude
10	Shirking	X	Integrity	Interne fraude
11	Single / Double moral hazard	X	Integrity	Interne fraude
12	Supplier employees have poor communication skills	X	Benevolence	Cliënten, producten en business

Van de 38 risico's benoemd door J. Tetteroo, lijken er dus 12 beïnvloedbaar te zijn via de vertrouwensfactoren.

Hierbij valt het op dat de 12 geselecteerde risico's, die door de onderzoeker geselecteerd zijn omdat deze verband houden met de factoren van trustworthiness, bijna allemaal vallen onder de twee categorieën: *Interne fraude* en *Cliënten, producten en business*.

5. Conclusies

5.1 Conclusie literatuuronderzoek

De onderzoeksvraag is er op gericht om te onderzoeken of de perceptie van IT-outsourcing risico's bewust te verminderen zijn aan de hand van factoren van vertrouwen en of hierop bewust te sturen is binnen je risicomanagement.

Tijdens het literatuuronderzoek zijn er meerdere modellen voorbijgekomen van vertrouwen binnen organisaties, echter het model van Mayer (1995) en zijn definitie van vertrouwen wordt breed gedragen binnen het vakgebied (bijvoorbeeld: (Heyns, 2015) (Lisa M. PytlikZillig, 2016).) Zijn model wordt zelfs gebruikt als basis en uitgebreid door andere onderzoekers (Andrew K. Schnackenberg, 2014). Het model is hierdoor ook gevalideerd door andere onderzoekers.

Mayer (1995) heeft een model opgesteld dat de trustworthiness weergeeft. In dit model zitten drie elementen:

- Ability (bekwaamheid, kundigheid)
- Benevolence (welwillendheid)
- Integrity (integriteit)

Het tweede belangrijke model wat naar voren is gekomen uit de literatuur is het consensus model van Earle. Dit model is door Earle opgesteld om vertrouwen te meten binnen risico management.

Het consensusmodel van Earle (2010) stelt dat er twee vormen van vertrouwen zijn:

Het relationele vertrouwen (trust), dat is gebaseerd op de relatie tussen personen / organisaties. Dit vertrouwen is breed gedragen, veerkrachtig en vooral bezig met intenties.

Het berekenend vertrouwen (confidence), dat is gebaseerd op gedrag uit het verleden en op beperkingen op het gedrag van de toekomst. Dit vertrouwen is vooral gebaseerd op specifiek gedrag en is kwetsbaar.

Earle benoemt tevens dat er Twee heuristieken zijn die van belang zouden kunnen zijn bij het beoordelen van vertrouwen; de *gelijkenis* heuristiek en de *invloed* heuristiek (Earle, 2010). De gelijkenis heuristiek is gericht op de waarden en intenties van de ander en de invloed heuristiek is gericht op het feit of er invloed kan uit geoefend kan worden op iemands gedragingen, want dan zal het vertrouwen hoger zijn.

Door middel van de heuristieken van Earle kunnen de drie factoren, ability, benevolence en integrity, van trustworthiness, beïnvloed worden om zo de trustworthiness te vergoten.

Elke relatie begint volgens (Rousseau, Sitkin, Burt, & Camerer, 1998) met calculatief vertrouwen, wat daarna langzaam overgaat in relationeel vertrouwen.

Rousseau stelt dat bij IT- outsourcing twee contracten behoren, namelijk het formele contract en het psychologische contract. Vertrouwen is onderdeel van het psychologische contract.

Information Technologie Outsourcing (ITO), is het uitbesteden van IT bezittingen, resources aan activiteiten aan een derde partij (Urbach & Wurz, 2012).

Het concept van een psychologisch contract is zeer relevant voor de context van IT- outsourcing. In feite is de focus op het niveau van het individuele gebruik van psychologische contracten dat zorgt voor een unieke en tot nu toe weinig bestudeerd perspectief op de relaties die ontstaan tussen organisaties tijdens outsourcing (Koh, 2004). De wederkerigheid van het psychologische contract is te koppelen aan de factor benevolence (welwillendheid) van trustworthiness zoals Mayer deze beschrijft. Want een psychologisch contract bestaat alleen als beide partijen van mening zijn dat een overeenkomst bestaat, dat de gemaakte afspraken zijn gemaakt en die overwegingen in ruil zijn aangeboden (Rousseau, 2001). Daarnaast kan de wederkerigheid ook gekoppeld worden aan de gelijkenis heuristiek (gelijkenis van waarden en intenties tussen partijen) van Earle (2010), want volgens het psychologisch contract betekent wederkerigheid in wezen " dat de partijen die betrokken zijn in feite te houden zijn aan dezelfde opvattingen ten aanzien van hun verplichtingen jegens elkaar " (Rousseau, 2001)(Koh, 2004).

Door de onderzoeker zijn 12 ITO risico's geïnterpreteerd in dit literatuuronderzoek. Bij de selectie is door de onderzoeker gekeken welke factor van vertrouwen (Integrity, benevolence, ability (Mayer, 1995)), dit risico beïnvloed en onder welk gedragsrisico deze onder te verdelen is (Aung, 2008).

5.2 Voortuitblik voor het empirisch onderzoek

In dit literatuuronderzoek is het bewust sturen van factoren van vertrouwen om risico's te reduceren niet gevonden in de onderzochte literatuur. Er is veel binnen de literatuur onderzocht met betrekking tot vertrouwen en risico management, maar binnen dit literatuuronderzoek is er niets gevonden over het bewust sturen van factoren van vertrouwen. Dit zou mogelijk in een vervolgonderzoek onderzocht worden waarbij de 12 geselecteerde ITO risico's als basis kunnen dienen.

De onderzoeker wil zowel het model van Earle als het model van Mayer gebruiken voor een vervolgonderzoek. Door het gebruik van beide modellen, Earle en Mayer, wil de onderzoeker beiden studiegebieden bij elkaar brengen: het model van Mayer gebaseerd op de drie factoren van trustworthiness (organisatie vertrouwen) en het consensus model van Earle (vertrouwen in risicomanagement).

Door deze twee gebieden bij elkaar te brengen kan een nieuw model ontstaan die vanuit beide modellen opgesteld kan worden. Een vervolgonderzoek zou kunnen zijn om dit model te gaan ontwikkelen.

De mogelijkheden om de onderzoeksvraag te beantwoorden kunnen tweeledig zijn, vanuit het perspectief van de leverancier en vanuit het perspectief vanuit de klant. De klant kan zijn potentiële leverancier uitkiezen op bepaalde elementen van vertrouwen en de leverancier kan zijn gedrag aanpassen aan de klant zodat deze meer vertrouwen heeft of krijgt in de (potentiële) leverancier. In dit literatuuronderzoek is deze richting open gelaten, deze richting kan worden gekozen binnen het empirisch onderzoek en bij de keuze van het uiteindelijk te kiezen instrument voor het onderzoek.

6. Referenties

- Al-Natour S, B. I., Cefetelli RT. . (2008). The effects of process and outcome similarity on users. *Decision Sciences*, 39(2), 175-211.
- Aung, Z. Z. (2008). Operational Risk Management Framework for service outsourcing: Consideration of risk dimensions and their application into the framework. *International Journal of Electronic Business Management*, 6(3), 120-130.
- Bachmann, R. (2001). Trust, Power and Control in Trans-Organizational Relations. *Organization Studies*, 22(2), 337–365.
- Bill McEvily, M. T. (2011). Measuring trust in organisational research: Review and recommendations. *Journal of trust research*, 23-63.
- Chrysoschoidis G, S. A., Krystallis A. (2009). Public trust in institutions and information sources regarding risk management and communication: Towards integrating extant knowledge. *Journal of Risk Research*, 12(2), 137-185. doi:10.1080/13669870802637000
- Das, T. (2001). Trust, Control, and Risk in Strategic Alliances: An Integrated Framework. *Organization Studies*, 22(2), 251–283.
- Earle, T. C. (2004). Thinking aloud about trust. *Risk Analysis*, 24(1), 169-183.
- Earle, T. C. (2010). Trust in Risk Management: A Model-Based Review of Empirical Research. *Risk Analysis*, 30(4), 541-574.
- Gill, H. (2005). Antecedents of trust: Establishing a boundary condition for the relation between propensity to trust and intention to trust. *Journal of Business and Psychology*, 19(3), 287-302.
- Heiskanen, A. (2008). Control, trust, power, and the dynamics of information system outsourcing relationships: A process study of contractual software development. *Journal of Strategic Information Systems*, 17, 268-286.
- Heyns, M., & Rothmann, S. . (2015). Dimensionality of trust: An analysis of the relations between propensity, trustworthiness and trust. *A Journal of Industrial Psychology/SA Tydskrif vir Bedryfsielkunde*, 41(1263).
- Inkpen, R. B. a. A. C. (2011). Understanding Institutional- based Trust Building Processes in Inter-organizational Relationships. *Organization Studies*, 32(2), 281-301. doi:10.1177/0170840610397477
- Kadabade, A. (2000). critical review - outsourcing: a paradigm shift. *Journal of Management*, 19(8), 670-728.
- Kavan, S. M. M. a. B. (2005). Moments of governance in IS outsourcing: conceptualizing effects of contracts on value capture and creation. *Journal of Information Technology*, 20, 152-169.
- Koh, C. S., Ang Straub, Detmar W. (2004). IT Outsourcing Success: A Psychological Contract Perspective. *Information Systems Research*, 15(4), 356-373. doi:10.1287/isre.1040.0035
- Langfield-Smith, K. a. D. S. (2001). *Management and control of outsourcing relationships : Evidence from the electricity industrie*.
- Lisa M. PytlikZillig, J. A. H., Ellie Shockley, Mitchel N. Herian, Tess M.S. Neal, Christopher D. Kimbrough, Alan J. Tomkins & Brian H. Bornstein. (2016). The dimensionality of trust-relevant constructs in four institutional domains: results from confirmatory factor analyses. *Journal of Trust Research*. doi:10.1080/21515581.2016.1151359
- Mass Soldal Lund, B. S., Ketil Stolen. (2010). Evolution in Relation to Risk and Trust Management. 5, 1, 49-55. doi:<http://doi.ieeecomputersociety.org/10.1109/MC.2010.134>
- Mayer, R. C., Davis, J. H., & Schoorman, F. D. . (1995). An integrative model of organizational trust. *Academy of management review*. 20(3), 709-734.
- Nooteboom, B. (2000). Trust as a Governance Device. In M. C. a. A. Godley (Ed.), *Cultural Factors in Economic Growth* (pp. 44-68): Springer Berlin Heidelberg.

- Rosalinde Klein Woolthuis, B. H. a. B. N. (2005). Trust, Contract and Relationship Development. *Organization Studies*, 813-840.
- Rousseau, D. M. (2001). Schema, promise and mutuality: The building blocks of the psychological contract. *Journal of Occupational & Organizational Psychology*, 74(4), 511.
- Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-disipline view of trust. *Academy of Management Review*, 23(3), 393-404.
doi:10.5465/AMR.1998.926617
- Saunders M., L., P and Thornhill, A. . (2015). *Methoden en technieken van onderzoek*. Amsterdam: Pearson Benelux
- Siegrist, T. C. E. a. M. (2006). Morality Information, Performance Information, and the Distinction Between Trust and Confidence. *Journal of Applied Social Psychology*, 36(2), 383-416.
- Tetteroo, J. (2016). *De risico's van IT outsourcing en IT co-sourcing vergeleken, literatuurstudie BPMIT*. Open Universiteit.
- Tomkins, C. (2001). Interdependencies, trust and information in relationships, alliances and networks. *Accounting, Organizations and Society*, 26, 161-191.
- Urbach, N., & Wurz, T. (2012). How to steer the IT outsourcing Provider. *Business & Information systems engineering*, 5, 247-259.

7. Bijlagen literatuuronderzoek

7.1 Bijlage 1 literatuuronderzoek: Lijst van tertiaire bronnen waarbinnen gezocht is

- Academic Search Elite (EBSCO)
- ACM Digital Library
- Business Source Premier (EBSCO)
- Cambridge Journals
- DOAJ - Directory of Open Access Journals
- EBSCO Host
- E-Journals (EBSCO)
- Emerald [management plus]
- ERIC (EBSCO)
- Google Scholar / Google Wetenschap
- GreenFILE (EBSCO)
- HeinOnlineIEEE Digital Library
- JSTOR Business, Biological, Mathematics & Statistics Collection
- Kluwer Navigator | kies: 'login voor WO/HBO'
- Lecture Notes in Computer Science
- Legal Intelligence
- Library, Information Science & Technology Abstracts - LISTA (EBSCO)
- LiteRom Jeugd
- LiteRom Nederlandstalige Literatuur
- LiteRom Wereldliteratuur
- NARCIS - the Gateway to Dutch Scientific Information
- Nature : international weekly journal of science
- OpMaat Premium
- Overheid.nl
- Oxford Journals
- PsycArticles (EBSCO)
- Psychology and Behavioral Sciences Collection (EBSCO)
- PsycINFO (EBSCO)
- PubMed
- Regional Business News (EBSCO)
- SAGE Journals
- Science
- ScienceDirect (Elsevier)
- SpringerLink
- Taylor & Francis Online
- Web of Science
- Wiley Online Library
- WorldCat

7.2 Bijlage 2 literatuuronderzoek: overzicht gebruikte artikelen, tijdvakken, aantal keren geciteerd en bron

Auteurs

In totaal hebben 60 unieke auteurs meegewerkt aan de gebruikte artikelen, van alle auteurs hebben R. Bachman en D. M. Rousseau meegewerkt aan twee artikelen, heeft T.C. Earle meegewerkt aan drie artikelen en de overige auteurs worden telkens één maal genoemd als auteur.

Tabel 5: *Artikelen per tijdvak*

Tijdvak	Aantal artikelen
1995 - 1999	2
2000 - 2004	9
2005 - 2009	8
2010 - 2016	8
Totaal	27

Tabel 6: *Aantal keren dat de gebruikte artikelen zijn geciteerd (per 19 september 2016)*

Minimum: 0

Maximum: 14.647

Aantal keren geciteerd	Aantal artikelen
0- 49	7
50- 99	5
100 - 499	8
500- 999	3
1.000- 5.000	2
5.000– 10.000	1
10.000 – 15.000	1
Totaal	27

Tabel 7: *Aantal artikelen per tertiaire bron*

Tertiaire bron	Aantal artikelen
EBSCO host - Business Source Premier	3

Google scholar	6
Emerald Insight	1
IEEE	1
JSTOR	2
Sage Journals	4
SAJP	1
ScienceDirect (Elsevier)	2
Springer	2
Taylor & Francis	2
Wiley Online Library	3
Totaal	27

7.3 Bijlage 3 literatuuronderzoek: Resultaten risicoanalyse

Resultaten van de risicoanalyse van het literatuuronderzoek van Jeroen Tetteroo. (Tetteroo, 2016)

Risico	Van toepassing volgens literatuur			Van toepassing volgens eigen analyse	
	ITO	ITC	BPO	ITO	ITC
Backlash from internal IT staff	✓	✓	?	✓	✓-
Business uncertainty	✓	?	?	✓	X
Complexity of business processes	?	?	✓	✓	X
Contractual risks	✓	✓	?	✓	✓
Coordination between client and vendor	✓	?	✓	✓	✓
Cultural differences between client and supplier	✓	✓	?	✓	✓-
Data losses and insufficient recovery	✓	?	?	✓	✓-
Difficulty in managing remote teams	✓	?	?	✓	X
Excessive transaction costs	✓	?	?	✓	✓-
Hidden costs	✓	✓	?	✓	✓
Incompatible systems, software and procedures	✓	?	?	✓	✓-
Inflexibility regarding business change	✓	?	?	✓	✓-
Lack of organizational learning	✓	?	?	✓	X
Lack of personalization functionality	✓	?	?	✓	X
Lack of trust	✓	✓	?	✓	✓
Loss of autonomy and control over IT decisions	✓	?	?	✓	X
Loss of control over data	✓	?	?	✓	✓-
Loss of in-house capability	✓	✓	✓	✓	✓
Loss/infringement of intellectual assets	✓	?	?	✓	✓
No overall cost savings	✓	✓	?	✓	✓
Opportunistic behaviour	✓	?	?	✓	✓
Poor customer financial stability	✓	?	?	✓	✓
Poor supplier capability, service, financial stability	✓	✓	?	✓	✓
Possibility of weak management	✓	?	?	✓	✓
Regulatory violations	✓	?	✓	✓	✓-
Security/privacy breach	✓	?	✓	✓	✓
Service delivery problems	✓	?	?	✓	✓
Shirking	✓	?	✓	✓	✓-
Single/Double moral hazard	✓	?	✓	✓	✓-
Supplier employee turnover/burnout	✓	?	?	✓	✓
Supplier employees have poor communication skills	✓	?	?	✓	✓
Supplier goes out of business	✓	?	?	✓	✓
Supplier has too much power over the customer	✓	?	✓	✓	✓-
Technological complexity	✓	?	?	✓	X
Technological indivisibility	✓	?	?	✓	X
Transition failure	✓	?	?	✓	✓-
Treating IT as an undifferentiated commodity	✓	✓	?	✓	✓-
Uncontrollable contract growth	✓	?	?	✓	✓-

7.4 Bijlage 4 literatuuronderzoek: verantwoording selectiekeuze ITO risico's in verband met vertrouwen

Risico	Selectie eigen analyse			
	Van toepassing op vertrouwen	Motivatie m.b.t. Factor van vertrouwen van Mayer	Factor van vertrouwen van Mayer	Gedrag risico's van Aung + motivatie
Backlash from internal IT staff	X	Werknemers van de klant kunnen een vijandige houding aannemen richting de werknemers van de leverancier. Er is geen vertrouwen tussen beide partijen.	Integrity	<p>Werkgelegenheid en veiligheid op de werkplek</p> <p>Werknemers moeten in een veilige omgeving werken, zowel fysiek als psychisch.</p>
Business uncertainty	-	Dit risico gaat over dat de richting van de organisatie (klant) niet helder is. Dit heeft met de missie en strategie van deze organisatie te maken en niet met vertrouwen tussen klant en leverancier.		
Complexity of business processes	-	Dit risico gaat over de levering van sommige of alle IT-functies, waarbij een IT-functie onder andere een proces kan zijn. Dit heeft niets te maken met vertrouwen tussen klant en leverancier.		
Contractual risk	X	Zoals Kavan (2005) al stelde zijn er bij samenwerkingsrelaties drie vormen waar organisaties mee te maken krijgen, waarbij o.a. het psychologisch contract van Rousseau (1994) Hierin	Integrity, benevolence en ability	<p>Cliënten, producten en business</p> <p>Contracten zijn</p>

		speelt vertrouwen een rol.		onderdeel van de business en de afspraken met de leverancier.
Coordination between client and supplier	X	Optimale coördinatie tussen klant en leverancier kan de samenwerking vergemakkelijken. Goede relationele governance is een succes voor de samenwerking, vertrouwen tussen leverancier en klant speelt hierbij een rol	Integrity, benevolence en ability	Cliënten, producten en business Coördinatie tussen klant en supplier valt hieronder, dit punt slaat direct op cliënten en business
Cultural differences between client and supplier	X	De organisatorische cultuur van de klant sterk kan afwijken van die van de leverancier, dit kan betekenen dat de klant zich niet kan identificeren met de waarden / normen van de leverancier, waardoor hij minder betrouwbaar lijkt.	Integrity, benevolence	Cliënten, producten en business Dit punt valt onder dit risico omdat het de relatie tussen klant en leverancier betreft.
Data losses and insufficient recovery	-	Dit risico's betreft direct de data en hiermee de back up en recovery. Dit risico heeft geen relatie met vertrouwen.		
Difficulty in managing remote teams	X	Problemen die hierbij geschetst worden zijn het ontbreken van een gevoel van urgentie voor uit te voeren veranderingen door de fysieke afstand tussen teams, taalbarrières en culturele verschillen. Teams op afstand gaat veelal op basis van vertrouwen.	Integrity, benevolence	Cliënten, producten en business Dit punt valt onder dit risico omdat het de business en de veranderingen hierin betreft. Processen en werkafspraken in de business tussen remote teams.
Excessive	-	Dit risico gaat specifiek over kosten en		

transaction costs		heeft geen relatie met vertrouwen.		
Hidden costs	-	Dit risico gaat over kosten die van tevoren niet inzichtelijk zijn gemaakt. Dit risico heeft geen relatie met vertrouwen.		
Incompatible systems, software and procedures	-	Dit risico gaat over de systemen, software en applicaties en heeft geen relatie met vertrouwen.		
Inflexibility regarding business change	-	Dit risico gaat over de (in)flexibiliteit van de dienstverlener en de mate waarin deze kan veranderen. Dit risico heeft geen relatie met vertrouwen.		
Lack of organizational learning	-	De situatie waarin een organisatie niet in aanraking komt met nieuwe technologieën door de inzet van ITO. Dit risico heeft geen relatie met vertrouwen		
Lack of personalization functionality		Het gebrek aan mogelijkheden voor maatwerkfunctionaliteit, Dit risico heeft geen relatie met vertrouwen.		
Lack of trust	X	Als er geen vertrouwen is dan is de samenwerkingsrelatie niet succesvol.	Integrity, benevolence en ability	Clënten, producten en business Dit punt valt onder dit risico omdat het de relatie tussen klant en leverancier betreft.
Loss of autonomy and control over IT decisions	-	Dit risico gaat over controle en flexibiliteit over de IT beslissingen. Dit risico heeft geen relatie met vertrouwen.		
Loss of control over data	X	Dit risico gaat over dat data bij de concurrent terecht kan komen. Dit risico heeft een relatie met de integriteit van de leverancier.	Integrity, ability	Interne fraude Dit risico heeft een relatie met de integriteit van de leverancier en het

				personeel.
Loss of in-House capability	-	Dit risico gaat over verlies van kunde van de medewerkers. Dit risico heeft geen relatie met vertrouwen.		
Loss/infringement of intellectual assets	-	Dit risico gaat over verlies van kennisborging. Dit risico heeft geen relatie met vertrouwen.		
No overall cost savings	-	De besparingen op kosten blijven uit. Dit risico heeft geen relatie met vertrouwen.		
Opportunistic behaviour	X	De verwachtingen worden hoog gespannen. Optimistisch gedrag zorgt voor vertrouwen, terwijl het uitblijven van resultaten het verlies van vertrouwen inhoudt.	Integrity, benevolence	Interne fraude Dit risico heeft een relatie met de integriteit van de leverancier en het personeel.
Poor customer financial stability	-	De klant heeft geen stabiele financiële situatie. Dit risico heeft geen relatie met vertrouwen.		
Poor supplier capability, service, financial stability	-	De leverancier levert ondermaatse service. Dit risico heeft geen relatie met vertrouwen.		
Possibility of weak management	-	Zwak management zou de kosten kunnen laten stijgen wat kan resulteren in conflicten en onvrede. Dit risico heeft geen relatie met vertrouwen.		
Regulatory violations	-	Klant blijft verantwoordelijk voor de compliance. Daarbij moet leverancier wel voldoen aan wetgeving. Dit risico heeft geen relatie met vertrouwen.		
Security / privacy breach	X	Dit heeft met de integriteit van de leverancier en haar medewerkers te maken.	Integrity	Interne fraude Dit risico heeft een relatie met de

				integriteit van de leverancier en het personeel.
Service delivery problems	-	Beloofde service van de klant blijft uit. Dit risico heeft geen relatie met vertrouwen.		
Shirking	X	het opzettelijk ondermaats presteren en het verminderen van de geleverde service. Dit heeft met de integriteit van de leverancier te maken.	Integrity	Interne fraude Dit risico heeft een relatie met de integriteit van de leverancier en het personeel.
Single / Double moral hazard	X	Werken met dubbel moraal en shirking is hier onderdeel van. Dit heeft met de integriteit van de leverancier te maken.	Integrity	Interne fraude Dit risico heeft een relatie met de integriteit van de leverancier en het personeel.
Supplier employee turnover / burnout	-	Hoog verloop van personeel. Dit risico heeft geen relatie met vertrouwen.		
Supplier employees have poor communication skills	X	Slechte communicatie vanuit de leverancier is slecht voor het vertrouwen. Dit raakt de welwillendheid van de leverancier.	Benevolence	Cliënten, producten en business Slechte communicatie slaat hierbij op de communicatie over de producten en of procedures (business).
Supplier goes out of business	-	Dit risico betreft het faillissement van de leverancier en heeft geen relatie met vertrouwen.		

Supplier has too much power over the customer	-	Dit risico heeft te maken met de mate van macht dit de leverancier heeft op de klant en heeft geen relatie met vertrouwen.		
Technological complexity	-	Dit risico heeft te maken met de technologische complexiteit van de IT van de klant en of de leverancier hiervoor de kennis heeft. Dit risico heeft geen relatie met vertrouwen.		
Technological indivisibility	-	IT componenten zijn sterk afhankelijk van elkaar. Dit risico heeft geen relatie met vertrouwen.		
Transition failure	-	Dit risico heeft geen relatie met vertrouwen.		
Treating IT as an undifferentiated commodity	-	Dit risico heeft geen relatie met vertrouwen.		
Uncontrollable contract growth	-	Dit risico heeft te maken met het toenemen van het formele contract. Dit risico heeft geen relatie met vertrouwen.		

7.5 Bijlage 5 literatuuronderzoek: Dimensies van Vertrouwen

Dimensions of Trust (Bill McEvily, 2011)

	Dimension	Number of times operationalised
1.	Integrity	19
2.	Ability/competence	14
3.	Benevolence	14
4.	Affective	12
5.	Cognitive	11
6.	Trust (verbatim)	9
7.	Loyalty	7
8.	Openness	7
9.	Fairness	6
10.	Reliability	5
11.	Faith in intentions	4
12.	Predictability	4
13.	Promise/commitment fulfilment	4
14.	Willingness to risk	4
15.	Availability	3
16.	Consistency	3
17.	Discreteness	3
18.	Opportunism	3
19.	Receptivity	3
20.	Surveillance/monitoring	3
21.	Motives/intentions	2
22.	Avoids taking excessive advantage	1
23.	Calculative	1
24.	Character	1
25.	Communication	1
26.	Concern	1
27.	Coordination	1
28.	Credibility	1
29.	Dynamism	1
30.	Expertness	1
31.	Forbearance	1
32.	Goodwill	1
33.	Habitualisation	1
34.	Honesty	1
35.	Informal agreement	1
36.	Influence acceptance	1
37.	Institutionalisation	1
38.	Judgement	1

7.6 Bijlage 6 literatuuronderzoek: Modellen van vertrouwen binnen risicomangement

Onderstaande modellen zijn uitgewerkt in het artikel van Earle(2010).

TCC Model

Dit model is ontwikkeld door Earle and Siegrist. (Siegrist, 2006)

Het TCC model maakt een onderscheid tussen Trust en Confidence, waarbij beide, zowel afzonderlijk of gezamenlijk, kan leiden tot verschillende vormen van Coöperatie (samenwerking). Vertrouwen (Trust) is gebaseerd op de sociale relaties, of gedeelde waarden, met vermelding van goede bedoelingen naar de te vertrouwen persoon. De basis voor vertrouwen (Confidence) zijn de prestaties uit het verleden, of instellingen die ontworpen zijn om toekomstige prestaties te beheersen. Parallel aan algemeen vertrouwen, kunnen uitspraken van prestaties uit het verleden worden beïnvloed door algemeen vertrouwen, een neiging om zeker over de toekomst te zijn.

Net als in het consensusmodel onderscheidt het TCC model twee vormen van vertrouwen:

1. relationeel vertrouwen;
2. berekenend vertrouwen.

Consensusmodel

Het consensusmodel dat is ontwikkeld door Earle (2010) was in navolging van het Trust, Confidence en Cooperation- model (TCC) (Earle, Siegrist & Gutscher 2006). In het consensusmodel wordt er gesproken van relationeel en calculatief vertrouwen. In het TCC model wordt relationeel vertrouwen trust genoemd en calculatief vertrouwen confidence. In dit onderzoek wordt er verder alleen gesproken over de termen relationeel en calculatief vertrouwen.

Het consensusmodel maakt vooral onderscheid tussen intenties (relationeel vertrouwen) en competenties (calculatief vertrouwen) (Earle, 2010).

The Associationist model

Dit model van vertrouwen in risico management is gebaseerd op de relatie tussen Trust en technologie acceptatie, dit model is omgekeerd aan het consensus model. In dit model bestuurt technologie acceptatie zowel het vertrouwen als de perceptie van het risico, dit wordt "causal chain model" genoemd. Hierdoor heeft vertrouwen effect op risicomangement en risicomangement effect op technologie acceptatie.

The integrative model

Het integratieve model toont de belangrijkste elementen van het consensus model: het bevat zowel relationele en berekenende vormen van vertrouwen; het toont dat relationeel vertrouwen is gebaseerd op waarden gebaseerde heuristieken en het toont aan dat relationeel vertrouwen domineert aan berekenend vertrouwen.

Consumer Confidence model (CCM)

In dit model, is het vertrouwen gemeten langs twee dimensies, optimisme (voorbeeld: "Ik ben optimistisch over ") en pessimisme ("Ik maak me zorgen over") Beide concepten zijn emotionele aspecten maar zijn doorgaans berekenend. Het model bevat ook een concept genaamd vertrouwen, die wordt gemeten voor het grootste deel door relationele items ("... is eerlijk over de ").

Dit model identificeert zowel berekenend als relationeel vertrouwen, waarbij de laatste de eerste beïnvloedt. In dit opzicht is dit in overeenstemming met het consensus model.

Social Trust, Epistemic Trust, and Antagonism

Een recente studie van Sjöberg en Herber presenteert drie-trust gerelateerde factoren als verklarende variabelen, maar houdt geen rekening met een model van de relaties tussen deze variabelen.

Van het gezichtspunt gezien van het consensus model, is de toenadering die deze studie omvat een trust antecedent factor, een relationeel vertrouwen factor, en een berekenend vertrouwen factor. Deze drie factoren worden beschouwd als concurrerende variabelen ten opzichte van verschillende afhankelijke variabelen, echter niet als samenwerkende elementen in een geïntegreerd model van vertrouwen in risicomanagement.

7.7 Bijlage 7 literatuuronderzoek: Onderzoek naar meten van vertrouwen

Measure	Dimensions	Item generation process	Sample(s)	Reliability (Cronbach's Alpha)	Validity
McAllister (1995)	Cognition-based	1. Pooled existing items from literature	175 executive MBAs, each with two matched-peer dyads	Cognition-based=0.91 Affect-based=0.89	Convergent Discriminant Nomological
	Affect-based	2. Evaluated items by academic experts 3. Exploratory factor analysis			
Currall and Judge (1995)	Communicating openly and honestly	1. Derived four theoretical dimensions	154 matched dyads (school district superintendents, teachers' unions presidents)	Communication superintendents=0.72 presidents=0.71 Informal Agreement superintendents=0.73 presidents=0.68 Surveillance superintendents=0.79 presidents=0.82 Task Coordination superintendents=0.70 presidents=0.74	Convergent Discriminant Nomological
	Relying on informal agreements	2. Elicited items for dimensions via open-ended field interviews			
	Maintaining surveillance	3. Evaluated items with second group of field interviewees			
	Coordinating interdependent tasks				
Cummings and Bromiley (1996)	Good-faith efforts	1. Created new items based on protocol	323 MBA and Executive MBA students	Good-faith effort=0.95 Honesty in exchange=0.95	Convergence Nomological
	Honesty in exchange Limited opportunism	2. Reviewed for face validity by research group 3. Separate group of researchers sorted items into categories 4. Assessed discriminant validity versus commitment			
Mayer and Davis (1999)	Trustworthiness – Ability – Benevolence – Integrity	1. Generated preliminary set of items 2. Pilot tested on two groups	259 veterinary doctors 166, 170 and 193 production employees across three time periods	Ability=0.85 to 0.93 Benevolence=0.87 to 0.95 Integrity=0.82 to 0.96 Trust=0.59 to 0.82	Convergent Discriminant Nomological
	Trust			Also computed test-retest validity across different waves of data collection (0.75 and 0.66 between wave one and two and wave two and three respectively)	
Gillespie (2003)	Reliance	1. Derived two theoretical dimensions	88 matched leader-member dyads and	Reliance=0.90 to 0.92	Convergent Discriminant Nomological Cross-validation study with different sample.
	Disclosure	2. Field interviews validate dimensions 3. Generated preliminary set of items for each dimension 4. Pretested on two groups	39 matched peer dyads from personnel of large public R&D organisation	Disclosure=0.89 to 0.95	

11.3 Appendix 3: Motivering onderzoeksmethode

In deze appendix is de motivering voor de onderzoeksmethode opgenomen.

Methode	Beschrijving volgens Saunders (2015)	Toepasbaarheid op het onderzoek
Experiment	Het experiment is de klassieke vorm van onderzoek, die als doel heeft om causale verbanden te bestuderen, door na te gaan of een verandering in één onafhankelijke variabele een verandering teweegbrengt in een andere, afhankelijke variabele.	Dit onderzoek is niet op zoek naar bevestiging van bestaande causale verbanden en daarmee is een experiment niet toepassing voor dit onderzoek.
Surveyonderzoek	Een surveyonderzoek wordt vaak geassocieerd met de deductieve onderzoeksbenadering, en wordt het meest gebruikt om 'wie, wat, waar en hoeveel' vragen te beantwoorden.	<p>Dit onderzoek is een inductief onderzoek. Daarmee ligt het gebruik van de surveymethode niet voor de hand, maar zou wel toegepast kunnen worden.</p> <p>Dit onderzoek wordt uitgevoerd volgens het surveyonderzoek methode, omdat het onderzoek onderzoekt of de factoren van trustworthiness van Mayer (1995) een relatie hebben met twaalf ITO-risico's en wil tevens de sterkte van deze relatie vaststellen. In hoeverre hebben de factoren van trustworthiness een relatie met de twaalf ITO-risico's en hoe groot beïnvloedt deze relatie het totaal aan vertrouwen. Dit zal gebeuren door middel van interviews met experts op het desbetreffende gebied. De antwoorden zullen niet op basis van een bestaande case komen maar vanuit de ervaring van de expert.</p>
Casestudy	Een casestudy wordt omschreven als een methode voor het doen van onderzoek die gebruik maakt van een empirisch onderzoek van een bepaald hedendaags verschijnsel binnen de actuele context, waarbij van verschillende soorten bewijsmateriaal gebruik wordt gemaakt. De casestudy is vooral interessant indien men een goed begrip wilt krijgen van de	Het onderzoek is niet gebaseerd op casus binnen de organisaties, maar op basis van kennis en ervaring van de respondenten, daarmee past de casestudy strategie niet bij dit onderzoek.

	context van het onderzoek en de processen die worden doorlopen. Geschikt voor de 'Waarom, Wat en Hoe' vragen.	
'Action research'	<p>Bij de Action research houdt men zich bezig met het managen van een verandering en waarbij de mensen uit de praktijk en de onderzoekers nauw met elkaar samenwerken.</p> <p>Deze methode wordt gekenmerkt door vier thema's:</p> <ol style="list-style-type: none"> 1) Onderzoek in actie (in plaats van over actie). 2) Betrokkenheid van de mensen in de praktijk bij het onderzoek. 3) Herhaling in diagnosestelling, plannen, actie ondernemen en beoordelen. 4) Moet ook implicaties hebben buiten het directe project. <p>In het bijzonder geschikt voor 'hoe' vragen.</p>	Dit onderzoek betreft geen onderzoek in actie. De action research strategie past daarmee niet bij dit onderzoek.
'Grounded theory'	Hierin wordt de theorie ontwikkeld uit de gegevens door middel van een reeks waarnemingen of interviews, waarbij een voornamelijk inductieve benadering wordt gevolgd. Deze methode is vooral nuttig voor onderzoek waarin geprobeerd wordt om gedrag te voorspellen en te verklaren, waarbij de nadruk ligt op het ontwikkelen van theorie of een model. De theory kan gezien worden als 'het opbouwen van een theorie of model' door een combinatie van inductie en deductie.	Dit onderzoek is ingebed in een theoretisch kader en zal voortbouwen op het conceptueel model van Mayer. Daarmee is de grounded theory onderzoeksstrategie niet van toepassing op dit onderzoek.
etnografie	Deze methode heeft als doel het beschrijven en verklaren van de maatschappelijke wereld waarin de onderzochte personen leven, op de manier zoals zij die zouden beschrijven en verklaren.	Dit onderzoek richt zich niet op de hiernaast genoemde doelstellingen van etnografisch onderzoek: deze strategie is niet geschikt voor dit onderzoek.

11.4 Appendix 4: Gegevensverzamelingsformulier

In deze appendix is het semi-gestructureerde gegevensverzameling antwoord vel opgenomen.

Algemene informatie				
A.01	Verzoeknummer			
A.02	Datum			
A.03	Tijd (van tot)			
A.04	Locatie			
A.05	Verduidelijking opname van het interview			

Respondent	
A.06	Organisatie waar werkzaam
A.07	ICT beambtenaar
A.08	Functie
A.09	Organisatiebeheer
A.10	Kenmerk met ICT beambtenaar
A.11	Toetsnummer getuikel gegeven

Relatie TO-Hisco en factoren van Trustworthiness				
	Factoren van Trustworthiness	Ability (betrouwbaarheid)	Benewidence (veelwillendheid)	Integrity (integriteit)
A.12	TO-Hisco's			
A.12.1.1	Backlash from internal IT staff			
A.12.2.1	Contractual risk			
A.12.2.1	Contractual between client and supplier			
A.12.4.1	Cost of breach between client and supplier			
A.12.5.1	Difficulty in managing remote teams			
A.12.5.1	Lack of trust			
A.12.5.1	Loss of control over data			
A.12.6.1	Opportunistic behaviour			
A.12.9.1	Security / privacy breach			
A.12.10.1	Single / Double moral hazard			
A.12.12.1	Supplier employees have poor communication skills			

Factoren van Trustworthiness van toepassing op Backlash from internal IT staff				
A.12.1.2	Is de factor van Trustworthiness van toepassing op Backlash from internal IT staff			
A.12.2.2	Is de factor van Trustworthiness van toepassing op Contractual risk			
A.12.3.2	Is de factor van Trustworthiness van toepassing op Coordination between client and supplier			
A.12.4.2	Is de factor van Trustworthiness van toepassing op Difficulty in managing remote teams			
A.12.5.2	Is de factor van Trustworthiness van toepassing op Lack of trust			
A.12.6.2	Is de factor van Trustworthiness van toepassing op Loss of control over data			
A.12.7.2	Is de factor van Trustworthiness van toepassing op Opportunistic behaviour			
A.12.9.2	Is de factor van Trustworthiness van toepassing op Security / privacy breach			
A.12.10.2	Is de factor van Trustworthiness van toepassing op Single / Double moral hazard			
A.12.11.2	Is de factor van Trustworthiness van toepassing op Goal			
A.12.12.2	Is de factor van Trustworthiness van toepassing op Supplier employees have poor communication skills			

Invloed op het geheel van vertrouwen				
	Ability (betrouwbaarheid)	Benewidence (veelwillendheid)	Integrity (integriteit)	
A.13				
A.13.1				
A.13.1.1				
A.13.2.1				
A.13.3.1				
A.13.4.1				
A.13.5.1				
A.13.6.1				
A.13.7.1				
A.13.8.1				
A.13.9.1				
A.13.10.1				
A.13.11.1				
A.13.12.1				

Invloed op het geheel van vertrouwen				
	Ability (betrouwbaarheid)	Benewidence (veelwillendheid)	Integrity (integriteit)	
A.13				
A.13.1.2				
A.13.2.2				
A.13.3.2				
A.13.4.2				
A.13.5.2				
A.13.6.2				
A.13.7.2				
A.13.8.2				
A.13.9.2				
A.13.10.2				
A.13.11.2				
A.13.12.2				

Uitspraak

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

Cijfers van 0 tot en met 10 waarbij 0 geen invloed is en 10 heel veel invloed.

11.5 Appendix 5: Draaiboek interviews

In deze appendix is het draaiboek ten behoeve van het afnemen van de interviews opgenomen.

Formele vragen

- Dit gesprek wordt opgenomen, geeft u hier toestemming voor?
- Deelname van dit onderzoek is vrijwillig en indien u wilt stoppen kunt u dit te allen tijde aangeven.
- Stemt u toe om mee te werken aan dit onderzoek?
- De resultaten van dit interview worden anoniem verwerkt in een openbaar eindverslag. Geeft u toestemming om het resultaat van dit interview te verwerken in een openbaar eindverslag?

Introductie onderzoek

In dit empirisch onderzoek wordt de relatie gezocht tussen IT-outsourcing risico's en vertrouwen. Dit onderzoek is begonnen met een literatuuronderzoek. Dit literatuuronderzoek is gestart met als hoofdvraag: *"Hoe kunnen factoren van vertrouwen bewust ingezet worden om de perceptie van de risico's van IT-outsourcing te verlagen"*. Met andere woorden: Kan er bewust gestuurd worden op de perceptie van de hoogte van de risico's met als middel (factoren van) vertrouwen. In het literatuuronderzoek heeft de onderzoeker ITO risico's, die verband houden met vertrouwen, geselecteerd aan de hand van literatuur maar ook door middel van eigen interpretatie. Deze selectie wordt in het empirisch onderzoek getoetst. Om een antwoord te krijgen op de hoofdvraag van het literatuuronderzoek moet er eerst vast gesteld worden of er wel een relatie is tussen vertrouwen en ITO-risico's, want is er geen relatie dan kan er ook niet bewust gestuurd worden hierop. Daarnaast wordt er onderzocht wanneer er een relatie is, hoe sterk deze relatie is en hoe groot deze relatie van invloed is op het geheel aan vertrouwen.

Begrippen doornemen

Om te zorgen dat de begrippen hetzelfde geïnterpreteerd worden door de respondenten en de onderzoeker, is aan iedere respondent een lijst met begrippen toe gestuurd, welke in het interview gebruikt gaan worden. Deze begrippen worden tijdens het interview met de respondent besproken om zeker te zijn dat de begrippen begrepen zijn en dat alle respondenten op 1 lijn zitten. Tijdens het interview wordt er gevraagd of de begrippen helder zijn. Aan de respondent wordt gevraagd of deze de begrippen wilt uitleggen, of de respondent dit heeft meegemaakt in de praktijk en/of er een voorbeeld benoemt kan worden van elk risico.

Meetwaarde die gebruikt wordt tijdens het interview

Tijdens het interview worden een aantal stellingen benoemd. In hoeverre een factor van trustworthiness invloed heeft op het betreffende ITO-risico wordt via onderstaande Likertschaal vastgelegd.

De algemene vraag / stelling zal zijn; In hoeverre bent u het eens met de stelling dat de factor van toepassing is op het ITO-risico? Hierbij kan dan één van de onderstaande antwoorden op van toepassing zijn.

Likertschaal	
1	geheel oneens
2	oneens
3	neutraal
4	eens
5	geheel eens

Daarnaast zal er een rapportcijfer (van één tot tien) worden gevraagd met betrekking tot de invloed die de betreffende relatie zal hebben op het totale geheel van vertrouwen.

Voorbeeld vraag/antwoord

Bijvoorbeeld: Factor integriteit is van toepassing op ITO-risico X. Antwoord is: "Eens".

De invloed van de relatie van integriteit op dit ITO-risico op het totale geheel aan vertrouwen richting de leverancier is 9. Dit betekent dat integriteit een belangrijke rol speelt in het vertrouwen van de leverancier met betrekking tot dit ITO-risico.

11.6 Appendix 6: Begrippen onderzoek en interviews

In deze appendix zijn de begrippen ten behoeve van dit onderzoek opgenomen. Deze zijn ook als zodanig verstrekt aan de respondenten.

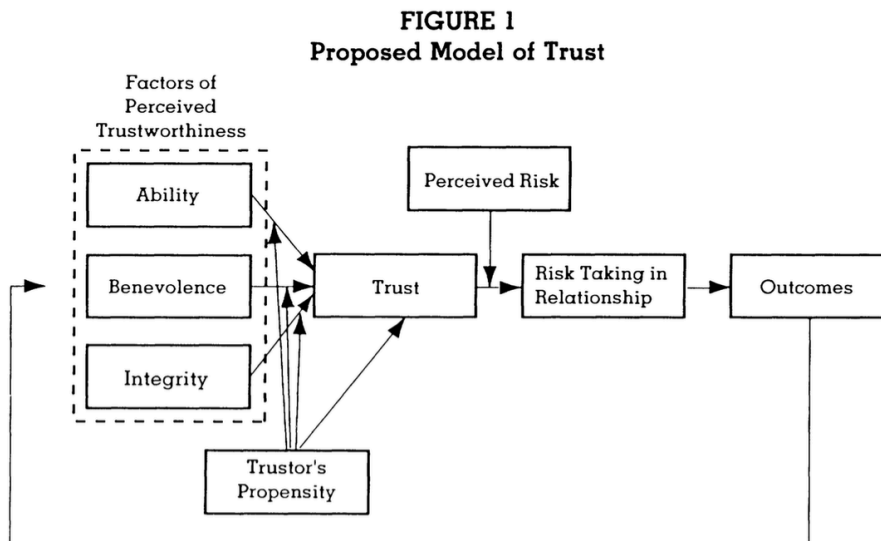
Begrippen

Om middels interviews te onderzoeken of er een relatie bestaat tussen vertrouwen en door de onderzoeker vooraf geselecteerde IT-Outsourcing risico's, is het noodzakelijk dat de begrippen binnen het onderzoek en interview helder zijn voor zowel de respondenten als de onderzoeker. Deze begrippen zijn hieronder weergegeven en zullen tijdens het interview besproken worden.

Het Model of Trust van Mayer stelt dat de drie factoren van trustworthiness, tezamen met de neiging van de *trustor* om zich kwetsbaar op te stellen, een bepaalde mate van vertrouwen weergeeft. Om de relatie tussen vertrouwen en de ITO risico's te bepalen worden binnen dit onderzoek de factoren van *trustworthiness* van Mayer (1995) gebruikt.

Vertrouwen:

"Vertrouwen is een psychologische toestand die de kwetsbaarheid accepteert op basis van positieve verwachtingen van de intenties of het gedrag van een ander"(Mayer, 1995).



Model of Trust (Mayer, 1995)

Factors of Trustworthiness

Ability (bekwaamheid)

Bekwaamheid is de groep van vaardigheden, competenties en karakteristieken die een partij in staat stelt om invloed uit te oefenen op een specifiek gebied.

Benevolence (welwillendheid)

Welwillendheid is de perceptie van de klant met betrekking tot de intentie van de leverancier om het goed te doen voor de klantorganisatie. Dit heeft niets te maken met een egocentrisch winstmotief. Welwillendheid is daarmee de perceptie van een positieve geste van de leverancier naar de klantorganisatie.

Integrity (integriteit)

Integriteit is de eigenschap dat iemand eerlijk en betrouwbaar is. Integriteit bestaat uit consistentie, eerlijkheid en openheid van de leverancier. De relatie tussen integriteit en vertrouwen houdt in dat de leverancier voldoet aan bepaalde principes die de organisatie acceptabel vindt.

IT-outsourcing risico's (ITO-risico's)

Backlash from internal IT staff

Een backlash (tegenwerking) komt vanuit de interne IT-medewerkers. IT-werknemers binnen de eigen organisatie moeten samenwerken met werknemers van de IT-leverancier die in de toekomst mogelijk hun baan zouden kunnen overnemen, omdat de interne IT-medewerkers overbodig zijn geworden. De interne werknemers kunnen hierdoor een vijandige houding aannemen, sturen op publieke bewustwording, of proberen politieke druk uit te oefenen. Indien interne IT-medewerkers geconfronteerd worden met organisatie brede verplaatsing van werk (IT-outsourcing), kan een backlash ook resulteren in intellectuele verlamming, productiviteitsverlies, stress en onzekerheid onder de medewerkers (Gartner, 2003). In beide gevallen gaat het om negatieve gevolgen naar aanleiding van het mogelijk verlies van banen of werkzaamheden bij ITO.

Contractual risk

Er kunnen veel problemen optreden met betrekking tot contracten, die samen te vatten zijn als contractuele risico's. Voorbeelden van deze risico's zijn:

- contractbreuk;
- inflexibele contracten;
- onenigheid omtrent de details van een contract;
- contractduur;
- onduidelijkheid met betrekking tot het resultaat van de door de dienstverlener uit te voeren processen;
- conflicterende en ongelijke doelen.

Coordination between client and supplier

Een effectieve coördinatie tussen de klant en de ICT- dienstverlener kan een goede samenwerking vergemakkelijken. Dit zou kunnen betekenen dat een minder optimale coördinatie een negatief effect kan hebben op de samenwerking, wat als een risico gezien moet worden. Coördinatie moet hierbij gezien worden als onderlinge afstemming tussen de klant en de leverancier. Het risico is dat er onderling geen goede (of onvoldoende) afstemming is tussen klant en leverancier.

Cultural differences between client and supplier

Ondanks uitgebreide selectietrajecten, wordt het cultuurverschil tussen de partijen (klant en leverancier) vaak benoemd als een hindernis voor verbetering van de samenwerking. De culturele ('zachte') aspecten zijn vaak onderbelicht of worden overschaduwd door de 'harde' aspecten. De focus ligt nog te veel op processen, contracten en SLA's, terwijl het in de relatie met de business veel meer gaat over de ontwikkelingen die er bij de klant spelen en de wijze waarop je daarmee omgaat in de samenwerking. Hoe zorg je ervoor dat het 'DNA' matcht met dat van de organisatie?

Difficulty in managing remote teams

Dit risico is voornamelijk van toepassing op *offshoring* (outsourcing in een gebied dat ver weg ligt,

bijv. India) en softwareontwikkeling met behulp van virtuele teams. Problemen die hierbij geschetst worden zijn het ontbreken van een gevoel van urgentie voor uit te voeren veranderingen door de fysieke afstand tussen teams. Tevens worden taalbarrières en culturele verschillen hierbij ook benoemd.

Lack of trust

De meest gangbare definitie van vertrouwen is:

“Vertrouwen is een psychologische toestand die de kwetsbaarheid accepteert op basis van positieve verwachtingen van de intenties of het gedrag van een ander.” (Mayer, 1995)

Vertrouwen wordt ook wel omschreven als “geloven dat de persoon die men vertrouwt zal doen wat men van hem verwacht”. Hierbij gaat het om het algehele vertrouwen wat de klant heeft in de IT-leverancier.

Vertrouwen is belangrijk voor het succes van IT-outsourcing. Indien dit vertrouwen ontbreekt is dit een risico voor de IT-outsourcing.

Loss of control over data

Verlies van data aan de concurrentie kan als een risico gezien worden. In theorie zou het kunnen voorkomen dat door verlies van controle over data, informatie van een klant bij een concurrent terecht komt. Logischerwijs vindt verlies van controle over data plaats indien bijvoorbeeld (een deel van) de infrastructuur wordt geoutsourcet naar een dienstverlener, waarbij de dienstverlener de infrastructuur overneemt. Ook als een dienstverlener vanaf een externe locatie beheer uitvoert over de systemen van de klant (of een extern datacenter heeft) kan dit risico plaatsvinden, alhoewel het risico mogelijk minder groot is door in plaats zijnde beveiligingsmaatregelen vanuit de klantorganisatie.

Opportunistic behaviour

Er zijn verschillende vormen van opportunistisch gedrag. In de masterthesis van Heuterman E.A. (2012) van de Vrije Universiteit Amsterdam, worden drie onderwerpen gedefinieerd: *shirking*, *free-riding* en *hold-up*.

Shirking

“Shirking” of *“Service debasement”* is het opzettelijk ondermaats presteren en het verlagen van de geleverde service of anders gezegd, het verlagen van de waarde, kwaliteit en / of status van de service die geleverd wordt.

Shirking is een actieve benadering, vergelijkbaar met jezelf verplaatsen binnen een groep vrienden in een bar, waarbij je probeert te vermijden om een rondje te geven. Het vermijden van contractuele verplichtingen, focussen op de korte termijn inkomsten, het opleggen van zoveel mogelijk kosten aan de joint venture zijn zakelijke voorbeelden hiervan.

Free-riding

Free-riding is passief, eigenlijk niets meer dan wachten tot de andere partners afspraken maken en hiervan vervolgens profiteren. Dit kan gemakkelijk worden gedaan als de bijdrage van de organisatie relatief klein is en het belang van de samenwerking voor de andere partners hoog is. Het beste moment om dit te voorkomen is in de onderhandelingsfase, hetzij door een betere omschrijving van de verplichtingen van elke partij, hetzij door ervoor te zorgen dat de samenwerking hetzelfde is voor alle partners. Uiteindelijk moet je free-riders zo veel mogelijk uitsluiten.

Hold-up

Hold-up is de meest strategische aanpak en gebaseerd op het benutten van de afhankelijkheid van de partner op de alliantie. Vergelijk het met uw loodgieter die komt met extra kosten op het moment dat de watertoevoer al is stilgelegd. Partners die deze benadering gebruiken proberen in de

contractuele fase afspraken open te laten. Grotere bedrijven hebben de neiging om dit te doen met (onvoorbereide) kleinere bedrijven.

Security / privacy breach

Dit risico heeft te maken met beveiliging en privacy gerelateerde risico's. Deze risico's staan hieronder in niet-limitatieve opsomming:

- Aanvallen op de verantwoordingsplicht;
- Aanvallen op authenticatie;
- Aanvallen op autorisatie;
- Aanvallen op beschikbaarheid;
- Aanvallen op vertrouwelijkheid;
- Aanvallen op integriteit;
- Gecompromitteerd vertrouwelijkheid van gegevens;
- Gecompromitteerde gegevensbeveiliging;
- Verlies van data;
- Openbaarmaking van gegevens door de provider;
- Host-based aanvallen;
- Onvoldoende verantwoording van de uitgevoerde acties;
- Onvoldoende bescherming van persoonsgegevens;
- Onvoldoende scheiding van naast elkaar bestaande gebruikers;
- Verlies van vertrouwelijkheid;
- Verlies van integriteit;
- Misbruik van gegevens door de provider;
- Netwerk-gebaseerde aanvallen;
- Onbeschermd gevoelige gegevens in de transmissie en opslag.

Als voorbeeld: een onbeveiligde USB-stick van de klant kan door een ITO-medewerker worden meegenomen en ITO-medewerkers zouden gevoelige gegevens naar een concurrent van de klant kunnen lekken.

Single / Double moral hazard

Moral hazard (Nederlandse termen zijn moreel risico, moreel gevaar en moreel wangedrag) is een economisch begrip dat verwijst naar veranderingen in het gedrag van partijen indien zij niet direct risico lopen voor hun daden.

In ITO-overeenkomsten zijn er altijd twee partijen: de klant en de dienstverlener. Een klant kan zaken doen met meerdere dienstverleners en vice versa, maar in de basis komt het neer op twee partijen die een overeenkomst met elkaar hebben afgesloten. Wanneer één van deze partijen zich niet optimaal inzet wordt dit een single moral hazard genoemd (Elitzur et al., 2012).

IT-outsourcing wordt gekenmerkt door de samenwerking tussen twee partijen waarbij beide partijen inspanning uitoefenen, dit niet waarneembaar is voor de andere partij. Dit kan uitmonden in een situatie waarbij er geen informatie wordt uitgewisseld terwijl dit wel relevant zou zijn. Aangezien de kwaliteit van het resulterende systeem afhankelijk is van de inspanning die beide partijen leveren kan dit leiden tot informatie asymmetrie, deze situatie wordt gekenmerkt als een *double moral hazard* (Elitzur et al., 2012).

Goal incongruence

Goal congruence betekent dat persoonlijke doelstellingen van de werknemers ook belangrijk zijn en dienen aan te sluiten bij de bedrijfsdoelstellingen. De belangen van zowel de organisatie als de werknemers moeten op één lijn komen te liggen om het beste uit de organisatie te halen. Het

nastreven van de doelstellingen van de organisatie en de werknemersdoelstellingen is een goede manier om alles uit je organisatie te halen. Het tegenovergestelde van goal congruence is goal incongruence.

Wanneer er sprake is van goal incongruence, namelijk dat niet alle neuzen één richting op staan, is dit een risico voor ITO. Indien de leverancier geen rekening houdt met de persoonlijke doelstellingen van de medewerkers van de klant is, het resultaat informatie-asymmetrie tussen klant en leverancier.

Supplier employees have poor communication skills

Bij dit risico gaat het over de communicatieve vaardigheden van de medewerkers van de leverancier. Indien deze vaardigheden ondermaats zijn, kan dit een risico vormen voor de samenwerking. Medewerkers van de IT-leverancier moeten communiceren met de klant. Wanneer dit niet op de juiste en een nette manier gebeurt kan hier miscommunicatie en zelfs schade door ontstaan.

Meetwaarde die gebruikt wordt tijdens het interview

Tijdens het interview worden een aantal stellingen benoemd. In hoeverre een factor van trustworthiness invloed heeft op het betreffende ITO-risico wordt via onderstaande Likertschaal vastgelegd.

De algemene vraag zal zijn; In hoeverre bent u het eens met de stelling dat de factor van toepassing is op het ITO-risico? Hierbij kan dan één van de onderstaande antwoorden op van toepassing zijn.

Likertschaal	
1	geheel oneens
2	oneens
3	neutraal
4	eens
5	geheel eens

Daarnaast zal er een rapportcijfer (van één tot tien) worden gevraagd met betrekking tot de invloed die de betreffende relatie zal hebben op het totale geheel van vertrouwen.

Bijvoorbeeld: Factor integriteit is van toepassing op ITO-risico X. Antwoord is: "Eens".

De invloed van de relatie van integriteit op dit ITO-risico op het totale geheel aan vertrouwen richting de leverancier is 9. Dit betekent dat integriteit een belangrijke rol speelt in het vertrouwen van de leverancier met betrekking tot dit ITO-risico.

11.7Appendix 7: Gegevensverzameling per respondent

In deze appendix zijn de gegevens opgenomen die per respondent zijn verzameld.

11.7.1 Respondent 1

Algemene informatie	
A.01	Respondentnummer 1
A.02	Datum 30-03-17
A.03	Tijd (van-tot) 13:00-15:00
A.04	Locatie Kantoor SZW Den Haag
A.05	Toestemming opname van het interview Ja

Respondent	
A.06	Organisatie waar werkzaam Inspectie Social Zaken en Werkgelegenheid
A.07	ICT leverancier Dienst Uitvoering ICT
A.08	Functie Informatiemanager
A.09	Werkzaamheden Contractmanagement, aansturing regelfunctie, vervanging accountmanagement, Gedelegeerd opdrachtgever.
A.10	Relatie met ICT leverancier Aanspreekpunt voor tactische samenwerking
A.11	Toestemming gebruik gegevens Ja

Relatie ITO-risico en factoren van trustworthiness				
Factoren van trustworthiness		Ability (bekwaamheid)	Benevolence (welwillendheid)	Integrity (integriteit)
A12	ITO-Risico's			
	Backlash from internal IT staff	4	4	4
	Contractual risk	5	5	5
	Coordination between client and supplier	4	5	5
	Cultural differences between client and supplier	4	4	4
	Difficulty in managing remote teams	5	4	1
	Lack of trust	5	5	5
	Loss of control over data	5	5	5
	Opportunistic behaviour	4	5	5
	Security / privacy breach	5	5	5
	Single / Double moral hazard	1	4	5
	Goal incongruence	1	4	2
	Supplier employees have poor communication skills	4	4	1

Invloed op het geheel van vertrouwen			
A.13	Ability (bekwaamheid)	Benevolence (welwillendheid)	Integrity (integriteit)
A.13.1.1	7	9	9
A.13.2.1	10	10	10
A.13.3.1	6	8	9
A.13.4.1	6	8	9
A.13.5.1	8	7	nvt
A.13.6.1	10	10	10
A.13.7.1	8	8	10
A.13.8.1	7	9	9
A.13.9.1	10	8	10
A.13.10.1	nvt	7	10
A.13.11.1	nvt	8	4
A.13.12.1	7	7	nvt

Appendices: Appendix 7: Gegevensverzameling per respondent

	Toelichting op de Likertwaarde	Ability	Benevolence	Integrity
A.1.2	Toelichting:	Toelichting:	Toelichting:	Toelichting:
			Omdat je niet weet hoe ze zich zullen gaan gedragen. Op het moment dat ze nu al aangeven dat ze niet welwillend staan tegenover de leverancier waar zij straks voor moeten werken, schaadt dat het vertrouwen wat je dan op dat moment hebt in de leverancier.	Indien de leverancier niet integer is ten opzichte van de bedoelingen m.b.t. Het interne IT leverancier van de klant, kan dit invloed hebben op het vertrouwen.
A.1.2.1.2	Is de factor van trustworthiness van toepassing op Backlash from internal IT staff?	Bekwaamheid van medewerkers kan invloed hebben. Goede lopen weg en de slechte blijven zitten, waardoor totale bekwaamheid naar beneden gaat. Met hoge bekwaamheid zijn ze beter in staat om bekwaam hun werk uit te voeren.		

Rapportcijfer	Ability	Benevolence	Integrity
A.1.3	Toelichting:	Toelichting:	Toelichting:
	Omdat ik denk dat je bekwaamheid ook een soort van patroon is dat je hebt. Op het moment dat je bekwaam bent en bekwaam handelt vanuit een professionele inslag dan kan je dat proberen te verhogen door het kennisniveau te verhogen, maar op het moment dat er andere factoren gaan spelen die sterker zijn, dan kan zelfs de meest bekwaame persoon alsnog eigenlijk besluiten om niet dat professionele gedrag te vertonen.	Omdat als je weet dat, dat de welwillendheid goed zit, dan heb je het vertrouwen dat ook in een nieuwe situatie, een onzekere situatie mensen er toch van alles er aan zouden blijven doen om voor jou de IT in orde te houden, zeg maar. En dat daar geen risico's optreden.	Zodra het gevoel bestaat dat de leverancier niet integer is dan neemt de backlash enorm toe.
A.1.3.1.2			

Appendices: Appendix 7: Gegevensverzameling per respondent

		Je wil het idee hebben dat ze op een professionele manier in staat zijn om als een goed huisvader zorg te dragen voor jouw data en daar geen fouten in te maken, dus bewust bekwaam is dat dan. Weten wat ze aan het doen zijn met de gegevens waar jij heel veel waarde aan hecht.	Dat zij aantonen dat zij het belang zien die jij hecht aan de data op dat moment.	Als je het gevoel hebt dat ze niet integer met je data omgaan, dan kun je het net zo goed niet plaatsen.
A.12.7.2	Is de factor van trustworthiness van toepassing op Loss of control over data			
		Op het moment dat je je welwillend bent in een relatie dat je zal beslissen geen opportunistisch gedrag te vertonen. Het zijn bijna twee tegenovergestelde dingen van elkaar.	En ja dan kom je echt in de fraudeachtige modellen. Ik ben nu doelbewust vanuit mijn onbetrouwbaarheid aan het zorgen om maximale uit het contract te slepen en je pakt eigenlijk alles aan om voor mij gunstig gedrag in te brengen.	
A.12.8.2	Is de factor van trustworthiness van toepassing op Opportunistisch behaviour	Op het moment dat je opportunistisch gedrag vertoont, op het moment dat je niet bekwaam bent tot wat je doet, dan kan dat juist leiden tot opportunistisch gedrag. Dus eigenlijk weet ik niet wat ik aan het doen ben, maar ik ben opportunistisch genoeg om me eruit te bluffen.		
		Ik denk dat de invloed niet zo heel groot is omdat je het vaak niet verwacht. Het is geen factor die heel duidelijk, nah ja ik denk er wel eens over na, weten ze nou heel anders goed waar ze mee bezig zijn om het optimale eruit te halen. Maar dan raakt je eigenlijk meer de integriteit ervan, dan ben je de boel aan het verliezen.	Het voorbeeld wat hier wordt gegeven; vergelijk het met de loodgieter die komt met extra kosten op het moment dat de watertoevoer al is stilgelegd. Partners die deze benadering gebruiken proberen in de contractuele fase dingen open te laten. Het lijkt alsof ze heel welwillend zijn, maar feitelijk maken ze gewoon totale misbruik van de situatie. Echte welwillendheid leidt niet tot opportunistisch gedrag.	Dan weet je zeker dat je het verlies aan controle over de data gaat ervaren en dat je de data als het ware vogelvrij wordt verklaard.
A.13.7.2				
A.13.8.2				

11.7.2 Respondent 2

Algemene informatie			
A.01	Respondentnummer	2	
A.02	Datum	04-04-17	
A.03	Tijd (van-tot)	10:00- 11:30	
A.04	Locatie	Kantoor Den Haag	
A.05	Toestemming opname van het interview	ja	

Respondent	
A.06	Organisatie waar werkzaam
A.07	ICT leverancier
A.08	Functie / rol
A.09	Werzaamheden
A.10	Relatie met ICT leverancier
A.11	Toestemming gebruik gegevens

Relatie ITO-risico en factoren van trustworthiness			
	Factoren van trustworthiness	Ability (bekwaamheid)	Benevolence (welwillendheid)
A12	ITO-Risico's		Integrity (integriteit)
A.12.1.1	Backlash from internal IT staff	4	4
A.12.2.1	Contractual risk	4	4
A.12.3.1	Coordination between client and supplier	2	4
A.12.4.1	Cultural differences between client and supplier	1	5
A.12.5.1	Difficulty in managing remote teams	4	4
A.12.6.1	Lack of trust	5	4
A.12.7.1	Loss of control over data	4	4
A.12.8.1	Opportunistic behaviour	4	5
A.12.9.1	Security / privacy breach	4	4
A.12.10.1	Single / Double moral hazard	3	4
A.12.11.1	Goal Incongruence	2	5
A.12.12.1	Supplier employees have poor communication skills	4	4

Invloed op het geheel van vertrouwen			
A13	Ability (bekwaamheid)	Benevolence (welwillendheid)	Integrity (integriteit)
A13.1.1	8	7	7
A13.2.1	8	6	7
A13.3.1	3	9	8
A13.4.1	nvt	9	7
A13.5.1	7	7	7
A13.6.1	8	7	7
A13.7.1	7	7	8
A13.8.1	7	9	9
A13.9.1	7	7	7
A13.10.1	6	7	8
A13.11.1	4	8	7
A13.12.1	8	8	8

Appendices: Appendix 7: Gegevensverzameling per respondent

Toelichting op de Likertwaarde	Ability	Benevolence	Integrity
A.12	Toelichting:	Toelichting:	Toelichting:
	De mate van tegenwerken hangt dus meer af van wat voor een consequenties het heeft voor de medewerkers, dan of we vrouwen hebben in de partij. Ik denk dat bekwaamheid heel belangrijk is, over het algemeenheid van de situatie van oke als mensen bijvoorbeeld over gaan naar de leverancier, wat ook een vorm van outsourcen is dan zullen ze de bekwaamheid, welwillendheid en integriteit van de leverancier wel belangrijk vinden, maar zeker de bekwaamheid.	Als ze wel bekwaam zijn, maar niet willen dan vind ik dat ook niet fijn.	
A.12.1.2	Is de factor van trustworthiness van toepassing op Backlash from internal IT staff?		
		Ja stel dat ze dus uiteindelijk minder welwillend blijken, maar wel bekwaam en integer wat is dan het effect.	Ja daar loop je dan wel weer risico, als ze op dit punt niet eerlijk blijken te zijn dan ja.
A.12.2.2	Is de factor van trustworthiness van toepassing op Contractual risk		
		De welwillendheid vind ik dan weer wel belangrijk en als dat uiteindelijk niet zo blijkt te zijn denk ik dat je ook een slechte coördinatie hebt.	Ik denk dat als die uiteindelijk minder blijkt te zijn dat je coördinatie dan ook niet lekker loopt.
A.12.3.2	Is de factor van trustworthiness van toepassing op Coordination between client and supplier		
A.12.4.2	Is de factor van trustworthiness van toepassing op Cultural differences between client and	Ook hier kan je natuurlijk risico lopen en heeft wat mij betreft ook veel minder met	Bij welwillendheid hoort dat je elkaar accepteert en dat

Rapportcijfer	Ability	Benevolence	Integrity
A13	Toelichting:	Toelichting:	Toelichting:
	Ja ik denk hetzelfde verhaaltje als daarnet, als mensen naar een andere organisatie toe moeten vinden ze het wel fijn als het een goede organisatie is. Dus als dat niet zo is dan gaan ze wel piepen, gaan ze sowieso wel. Als het een goede organisatie is da... ja dus het heeft zeker we invloed.		
A.13.1.2			
		Ik kan de mist in gaan als het contract niet goed in elkaar steekt.	Ik denk dat dan het risico minder is
A.13.2.2			
	Maar ik vind dat meer een relationeel aspect en dat vind ik minder bij ability en bekwaamheid horen. Maar daarom denk ik dat bekwaamheid daar minder invloed op heeft.		
A.13.3.2			
A.13.4.2		Nou ik denk dat als je welwillend bent dat, dat de	

Appendices: Appendix 7 : Gegevensverzameling per respondent

			Volgens mij gaat dit puur om de boel te belazeren. Dat is volgens mij puur een integriteit kwestie, maar aan de andere kant. Ze zijn dus veel minder welwillend dan gedacht, dus zo gezien loop je daar een risico. Met welwillend denk ik vooral aan de mate waarin mensen enthousiast zijn, maar de boel belazeren is echt een ander iets.	Nou ja hieruit blijkt, dat als ze zo gaan doen dat ze helemaal niet welwillend zijn en dat ze gewoon niet integer zijn.	
A.12.8.2	Is de factor van trustworthiness van toepassing op Opportunistic behaviour	Nah als je zo doet dan ben je niet bekwaam. Dus daar zit dan ook een relatie in.		Eigenlijk hetzelfde, ik zie hier niet veel verschil tussen de onderdelen van vertrouwen. Ik denk dat de security gewoon een combinatie is van welwillendheid, vaardigheid en integriteit. Alle factoren zitten erin.	
A.12.9.2	Is de factor van trustworthiness van toepassing op Security / privacy breach	Om de zaken goed te beveiligen moet je wel weten waar je mee bezig bent dus dat is zeker een vaardigheid. En dus als blijkt dat ze op dat punt minder scoren dan verwacht dan loop je daar een risico.	Ik denk dat je als je bij welwillendheid schijnt ook elkaars belangen te behartigen een rol en dat heeft hier ook voorrebben.		
A.12.10.2	Is de factor van trustworthiness van toepassing op Single / Double moral hazard	Ik denk dat niet zo zeer bekwaamheid met moraal te maken heeft.	Ik denk dat het een onderdeel van integriteit is dat als je ook gewoon voor een ander denkt		
A.13.8.2					nauw nemen, dus ik denk dat je hier meer risico loopt.
A.13.9.2					
A.13.10.2					

Appendices: Appendix 7 : Gegevensverzameling per respondent

			mee te maken en integriteit ook.	
A.12.11.2	Is de factor van trustworthiness van toepassing op Goal Incongruence	Ik denk dat dit vooral te maken heeft met welwillend, euh ook wel met integriteit, maar het minst met ability.	Ja het is ook een kwestie van gunnen, als je mensen naar een ander bedrijf gaan en je maakt daar afspraken over, je wilt natuurlijk als die mensen een doel hebben dat je dat dan ook meeneemt.	En integriteit in deze is natuurlijk ook belangrijk.
A.12.12.2	Is de factor van trustworthiness van toepassing op Supplier employees have poor communication skills	Ja weet je het woord vaardigheden geeft wat mij betreft aan dat het om ability gaat. En als ze de vaardigheden niet hebben, maar wel de welwillendheid, daarom lukt het niet.	Ze zijn misschien ook wel heel welwillend. Maar dat verdoezeld gebrek aan kwaliteit op dit vlak, als je er al naar had gekeken moet ik zeggen, want je neemt ook niet alles mee. Dus in die zin denk ik dat je een risico loopt op in ieder geval ability en ook op welwillendheid.	Want het kan ook zijn, dat ze het ook min of meer hebben verdoezeld,
A.13.11.2			Maar dat hangt ook af van de gunningsfactor. De welwillendheid van het bedrijf.	als dat niet klopt dan gaat het ook mis uiteindelijk, dan is de impact misschien iets minder.
A.13.12.2		Nah ik vind het wel een belangrijke vaardigheid, dus de impact is voor mij ook wel groot.		

11.7.3 Respondent 3

Algemene informatie	
A.01	Respondentnummer 3
A.02	Datum 06-04-17
A.03	Tijd (van-tot) 14:00-15:00
A.04	Locatie Den Haag, Kantoor
A.05	Toestemming opname van het interview Ja

Respondent	
A.06	Organisatie waar werkzaam Ministerie Sociale Zaken en Werkgelegenheid
A.07	ICT leverancier Shared Service Center-ICT
A.08	Functie Teamcoördinator
A.09	Werkaanheden Klant- advies- en leveranciersmanagement
A.10	Relatie met ICT leverancier leveranciersmanager
A.11	Toestemming gebruik gegevens Ja

Relatie TTO-risico en factoren van trustworthiness				
Factoren van trustworthiness		Ability (bekwaamheid)	Benevolence (welwillendheid)	Integrity (integriteit)
A12	ITO-Risico's			
	Backlash from internal IT staff	1	4	5
	Contractual risk	4	5	4
	Coordination between client and supplier	5	2	5
	Cultural differences between client and supplier	1	5	5
	Difficulty in managing remote teams	5	4	4
	Lack of trust	4	3	5
	Loss of control over data	5	1	5
	Opportunistic behaviour	1	4	5
	Security / privacy breach	5	3	4
	Single / Double moral hazard	1	5	4
	Goal incongruence	4	4	4
	Supplier employees have poor communication skills	5	4	1

Invloed op het geheel van vertrouwen			
A.13	Ability (bekwaamheid)	Benevolence (welwillendheid)	Integrity (integriteit)
A13.1.1	nvt	7	9
A13.2.1	8	8	8
A13.3.1	10	5	10
A13.4.1	nvt	9	10
A13.5.1	10	8	7
A13.6.1	9	7	10
A13.7.1	10	nvt	10
A13.8.1	nvt	8	9
A13.9.1	10	6	8
A13.10.1	nvt	10	8
A13.11.1	8	8	7
A13.12.1	10	8	nvt

Appendices: Appendix 7: Gegevensverzameling per respondent

Toelichting op de Likertwaarde		Ability	Benevolence	Integrity
A.12		Toelichting:	Toelichting:	Toelichting:
A.12.1.2	Is de factor van trustworthiness van toepassing op Backlash from internal IT staff?	Als je kijkt naar de backlash from internal IT staf die dus niet over gaat naar de leverancier, die in de toekomst mogelijk hun baan.. dat vind ik vooral iets emotioneels. En ik denk dat die eerder aanslaan op zaken als integrity en welwillendheid.	We hebben hier een situatie dat mogelijk de interne medewerkers over moeten naar de IT-leverancier, dat is een onzekere situatie, met een bepaalde mate van welwillendheid kun je een stukje van die onzekerheid wegnemen.	Dus de backlash reduceert, maar ik denk dat al mensen zien dat er echt integer gedrag vertoont wordt en het is nog concreetiseerd, wat dan verstaan wordt onder integrity, consistentie, eerlijkheid en openheid.
A.12.2.2	Is de factor van trustworthiness van toepassing op Contractual risk	Ik denk voor ability dat die er zeker wel is, want alles met contracten heeft voor een gedeelte te maken met inhoudelijke kennis rondom aanbestedingen en dergelijke en inhoudelijk ook de contracten die je met elkaar hebt afgesproken en de rechtsgeldigheid, de rolverdeling en hoe breed je dat hebt beschreven.	Bij de uitvoering van een contract helpt het heel erg voor de relatie als je voelt dat de ander wel van goede wil is.	Eerlijkheid en openheid natuurlijk. Je kan niet welwillend zijn en niet integer. Dat lijkt mij gewoon... een gekke combinatie.
A.12.3.2	Is de factor van trustworthiness van toepassing op Coordination between client and supplier	Daarbij is ability zeker belangrijk, want het gaat om vaardigheden, sociale vaardigheden onder andere en administratieve vaardigheden, die zijn daar wel van belang. Want als jij gewoon, we weten het allebei, netjes op tijd geïnformeerd wordt en dat je dus een betrouwbaar counterpart hebt, dan helpt dat al in de coördinatie.	Ja onder tijdsdruk of iemand is niet vaardig genoeg, nogmaals, die begrippen liggen natuurlijk wel erg in elkaars verlengde. Een welwillend iemand die niet capabel is die gun je misschien wel op persoonswaarde, wel oke ik kan niet boos op hem worden, maar je wordt er wel een beetje gek van.	Als jij onjuiste informatie krijgt of men komt zijn afspraken niet na, zonder dat dat te maken heeft met welwillendheid of betrouwbaarheid.
Rapportcijfer		Ability	Benevolence	Integrity
A.13		Toelichting:	Toelichting:	Toelichting:
A.13.1.2				En met name die openheid, dus transparantie, daar haal je die onzekerheden mee weg en daar dwing je ook respect mee af en daarom denk ik dat dat de grootste factor is om de backlash mee te reduceren.
A.13.2.2		Je moet echt verstand van zaken hebben om goed, gedegen en duidelijk een contract met elkaar af te stemmen om gedoe in de toekomst te voorkomen	Dus als je ziet dat de ander zijn best doet en om daar, goed naar je luistert en daarmee aan de slag te gaan.	Dus ik denk dat als mensen welwillend zijn dat ze dat vanuit een integer perspectief doen. Dus daarom denk ik dat in dit specifieke geval welwillendheid zwaarder weegt dan integriteit, omdat het in de slipstream zit.
A.13.3.2		Als dat goed werkt denk ik dat dat een tien is in de coördinatie, omdat dat namelijk er voor zorgt dat de informatie ongevraagd en zonder rappelleren naar je toe komt.	Waarom ik hem dan niet op 1 of 2 waardeer, omdat in de aanloop, dat je op basis van iemands welwillendheid niet gelijk het vertrouwen beschaaft, als je ziet dat iemand welwillend is, maar structureel wordt dat niks natuurlijk.	Dus die zou ik ook op vijf zetten en een 10, want dat gaat gelijk gedoe opleveren.

Appendices: Appendix 7: Gegevensverzameling per respondent

A.12.4.2	Is de factor van trustworthiness van toepassing op Cultural differences between client and supplier	Het heeft namelijk te maken met normen en waarden, culturele verschillen. En ik zie dan bekwaamheid zie ik daar minder dicht aan liggen als welwillendheid en zaken als openheid, eerlijk en consistentie.	Dat vind ik wel echt een cultureel aspect, dat heeft te maken met klantgerichtheid of je open stellen voor.	En integriteit is natuurlijk ook een belangrijk aspect, dat ligt zo dicht tegen de normen en waarden aan	
A.13.4.2				ik denk dat als iemand welwillend is dat die ook wil luisteren, dus van goede wil is	Als je cultuur definieert als de breed gedragen normen en waarden, en rituelen symbolen en alles wat erbij komt kijken, dan is welwillendheid gaat over intentioneel gedrag, maar integriteit dat zit dieper in het DNA van de organisatie en dus ook in jou als persoon. Dat stuurt veel meer de mate waarin je je gedrag ten toon spreidt. Bijvoorbeeld op zaken als consistentie, eerlijkheid en openheid in dit geval. Dus ik denk dat dit misschien nog wel meer van invloed is dan welwillendheid.

Appendices: Appendix 7: Gegevensverzameling per respondent

A.12.5.2	Is de factor van trustworthiness van toepassing op Difficulty in managing remote teams	Dan zijn al die factoren belangrijk als je het hebt over offshoring. Omdat namelijk, als een van die drie factoren onvoldoende is dan heb je veel minder mogelijkheden om dat onsite.. dus dit moet veel beter op orde zijn om die relatie goed te laten werken met een offshore team.	
A.13.5.2	Ik denk dat ability misschien nog wel het hoogste is, want je hebt vaak te maken met contractuele afspraken en met een soort werkpakket wat je offshore weg zet, een soort ontwikkelwerk en dat krijg je terug. Dan hangt het er heel erg van af hoe bekwaam iemand is om jou specs te vertalen bijvoorbeeld. Nah en als dat goed gaat denk je he dat beïnvloed mijn vrouwen, dat zijn wel bekwame mensen.	Je weet helemaal niet of ze welwillend zijn, misschien worden ze wel geslagen door hun baas, maar ze zitten in India, dus dat zie je niet.	En met name de consistentie is dan belangrijk.

Appendices: Appendix 7 : Gegevensverzameling per respondent

			<p>Welwillendheid misschien wel iets minder, maar vaardigheden denk ik wel, want vaardigheden bepaalt uiteindelijk toch in welke mate diegene levert wat je met hem hebt afgesproken. Iemand kan totaal niet welwillend zijn, omdat hij ruzie met zijn vrouw heeft of omdat hij niet zo lekker heeft geslapen, maar als hij toch elke keer zijn afspraken nakomt, dan heb ik toch vertrouwen in die persoon. Word ik niet blij van het feit dat ik voel dat hij niet zo welwillend is, maar ja dat beïnvloed dan minder dat aspect dan dat hij bekwam is.</p>		
A.12.6.2	Is de factor van trustworthiness van toepassing op Lack of trust		<p>Hier is integriteit natuurlijk het meest belangrijk, want ja dat triggert gelijk een lack of trust, as iemand niet integer is, niet eerlijk, niet open en niet consistent.</p>		
A.12.7.2	Is de factor van trustworthiness van toepassing op Loss of control over data	<p>als jou intentie is om geen verlies van data aan derden te veroorzaken dan moet jou ability hoog zijn, dus dan ben ik absoluut eens, zeker in een complexe infrastructuur</p>	<p>Welwillendheid, als je met de Beste wil van de wereld, het is veilig of niet, iemand is integer of niet, welwillendheid heeft daar weinig invloed op.</p>	Je moet wel eerlijk zijn	
A.13.6.2				<p>En waarom toch een zeven, ja als iemand dag in dag uit jaar in jaar uit niet welwillend is dan gaat het toch een beetje jeuken met je lack of trust. Want dan heb je namelijk elke keer zoiets van, wanneer gaat het om slaan</p>	
A.13.7.2					

Appendices: Appendix 7: Gegevensverzameling per respondent

A.12.8.2	Is de factor van trustworthiness van toepassing op Opportunistic behaviour	En waarom er zit iets opzettelijks in, dus dat heeft wat mij betreft niet zo veel met.. ja je moet wel de vaardigheden hebben om niet integer te handelen of opportunistisch te handelen, maar dat is volgens mij niet de doelstelling van dit risico.	Shirking heeft echt met welwillendheid te maken, het opzettelijk ondermaats presteren, je wil dus eigenlijk gewoon niet.	Maar hij heeft ook een aspect met eerlijkheid, dus het is een combinatie van welwillendheid en integriteit
A.12.9.2	Is de factor van trustworthiness van toepassing op Security / privacy breach	Nou hier is nou net ability, vaardigheden, wel belangrijk, want het is echt een vak om complexe omgeving veilig te houden.	Als iemand niet welwillend is dan heeft dat invloed op zijn motivatie en dan zakt toch zijn aandacht niveau en dan heeft dat toch effect op..	En iemand kan heel bekwaam zijn, maar als hij niet integer is dan heb je kans dat hij zijn bekwaamheid gaat inzetten voor andere dingen. Die gelijk he vertrouwen beschadigen.
A.12.10.2	Is de factor van trustworthiness van toepassing op Single / Double moral hazard	dat vind ik minder relevant	Er staat hier ook als een van de partijen zich niet optimaal inzet, wat mij betreft een op een welwillendheid	Omdat het ook iets oneerlijks heeft, een beetje free-ride-achtige aspect.
A.12.11.2	Is de factor van trustworthiness van toepassing op Goal Incongruence	Dat heeft met vaardigheden te maken, is iemand in staat om dat te zien, om het aan te voelen en om er adequaat mee om te gaan.	Hetzelfde geldt voor welwillendheid, die leverancier moet natuurlijk wel bereid zijn om dat te zien en daar de voordelen van eens. Ja ik moet dat reduceren en mee dealen.	En het heeft volgens mij dan dan niet zo veel met integriteit te maken, omdat je het functioneel ziet, van ik weet dat er naast bedrijfsdoelstellingen ook persoonlijke doelstellingen zijn, daar moet ik in mijn relatie met mijn afnemer rekening mee houden, ja dat heeft wel iets met integriteit te maken. Je moet hem ook niet op lager
A.13.8.2				Je moet wel bekwaam zijn om free-ride gedrag te vertonen, maar goed dat komt vooral voort uit beperkt integer gedrag en de welwillendheid om dat gedrag te vertonen.
A.13.9.2				Vanwege de inhoudelijke kennis die nodig is en die als iemand kan aantonen dat die zoveel verstand van zaken heeft dan beïnvloed dat mijn vertrouwen. Neem bijvoorbeeld een Koos, als ik bij hem het gevoel krijg, ik ken de materie door en door en ik heb allemaal soorten cursussen gevolgd en ik heb er ervaring mee en ik weet hoe we al die aspecten en aanvallen moeten tackelen. Dan vind ik zijn welwillendheid en zijn integriteit helemaal niet.. minder relevant voor onze vertrouwensrelatie. Als hij als autoriteit, want daar gaat het dan om. Autoriteit en dat zie ik dan vooral voor bekwaamheid en natuurlijk heeft dat ook iets te maken met integriteit, die zou ik ook vooral niet op een zetten.
A.13.10.2				Hoewel dat natuurlijk ook wel te maken heeft met een stukje eerlijkheid
A.13.11.2				integriteit is gelimiteerd tot drie, consistente, eerlijkheid en openheid van de leverancier

Appendices: Appendix 7: Gegevensverzameling per respondent

				dan drie zetten.			
A.12.12.2	Is de factor van trustworthiness van toepassing op Supplier employees have poor communication skills	Dit heeft natuurlijk een op een met vaardigheden te maken, het gaat om skills.	En ability en welwillendheid, die dekken het willen en het kunnen.	Ja in relatie tot die communication skills, dat vind ik dat lastig te interpreteren, gevoelsmatig zou ik hem zelfs helemaal op 1 zetten, als je echt naar skills kijkt. En weet je waarom? Oplichters die kunnen vaak perfect communiceren, waarom? Dat is voor hun heel erg belangrijk om hun doel te bereiken. Dat zegt niks over hun integriteit, het zegt wel iets over het feit dat ze heel gemotiveerd zijn om het te doen en dat ze ook de vaardigheid			
A.13.12.2			Om het echt te kunnen toepassen, communicatie vaardigheden, dan moet je het willen en kunnen.	Om het echt te kunnen toepassen, communicatie vaardigheden, dan moet je het willen en kunnen.			

11.7.4 Respondent 4

Algemene informatie			
A.01	Respondentnummer		R4
A.02	Datum		09-05-17
A.03	Tijd (van-tot)		10:00-11:00
A.04	Locatie		Thuis
A.05	Toestemming opname van het interview		nvt

Respondent	
A.06	Organisatie waar werkzaam
A.07	ICT leverancier
A.08	Functie
A.09	Werkzaamheden
A.10	Relatie met ICT leverancier
A.11	Toestemming gebruik gegevens

Relatie ITO-risico en factoren van trustworthiness			
Factoren van trustworthiness		Ability (bekwaamheid)	Benevolence (welwillendheid)
A12	ITO-Risico's		Integrity (integriteit)
	A.12.1.1	Backlash from internal IT staff	1
	A.12.2.1	Contractual risk	5
	A.12.3.1	Coordination between client and supplier	5
	A.12.4.1	Cultural differences between client and supplier	5
	A.12.5.1	Difficulty in managing remote teams	5
	A.12.6.1	Lack of trust	5
	A.12.7.1	Loss of control over data	5
	A.12.8.1	Opportunistic behaviour	1
	A.12.9.1	Security / privacy breach	5
	A.12.10.1	Single / Double moral hazard	1
	A.12.11.1	Goal incongruence	4
	A.12.12.1	Supplier employees have poor communication skills	5

Invloed op het geheel van vertrouwen			
A.13	Ability (bekwaamheid)	Benevolence (welwillendheid)	Integrity (integriteit)
A.13.1.1			8
A.13.2.1		9	7
A.13.3.1		9	9
A.13.4.1		8	9
A.13.5.1		9	6
A.13.6.1		10	6
A.13.7.1		10	10
A.13.8.1		10	7
A.13.9.1		10	8
A.13.10.1		10	5
A.13.11.1		6	8
A.13.12.1		10	9

11.8 Appendix 8: Transcriptie interviews per respondent

In deze appendix is de transcriptie opgenomen van de interviews met de respondenten.

Deze appendix bevat de geanonimiseerde interviewtranscripties. Geanonimiseerd betekent dat de namen van respondenten, bedrijven, producten projecten en locaties niet zijn opgenomen in de transcriptie.

11.8.1 Respondent 1

1. Formele vragen bij start van het interview

Opmerking: dit is een gestandaardiseerde tekst en geen letterlijke transcriptie. De onderzoeker leest onderstaande vragen voor:

- Dit gesprek wordt opgenomen, geeft u hier toestemming voor?
- Deelname van dit onderzoek is vrijwillig en indien u wilt stoppen kunt u dit te allen tijde aangeven. Stemt u toe om mee te werken aan dit onderzoek?
- De resultaten van dit interview worden anoniem verwerkt in een openbaar eindverslag. Geeft u toestemming om het resultaat van dit interview te verwerken in een openbaar eindverslag?

2. Introductie onderzoek

Hier wordt door de onderzoeker het onderzoek uitgelegd. Niet getranscribeerd.

3. Begrippen doornemen

De begrippen zoals deze zijn toegestuurd voor aanvang van het onderzoek worden met de respondent besproken. Aan de hand hiervan stelt de onderzoeker vast dat de begrippen overeenkomen met de visie van de respondent over deze begrippen. Niet getranscribeerd.

4. gegevensverzameling

De wijze van vragen stellen en te geven antwoorden worden met de respondent besproken en de onderzoeker geeft een voorbeeld van een vraag/antwoord. Niet getranscribeerd.

Vanaf het moment dat de vragen met betrekking tot de relatie tussen de factoren van trustworthiness en de ITO-risico's worden gesteld is het letterlijk getranscribeerd.

O: Is onderzoeker

R2: Is respondent 1

O: Is de factor van trustworthiness, euhm... even kijken... is de factor ability

R1: Bekwaamheid, ja

O: Ja, van toepassing op backlash from internal IT staf?

R1: Euhm...

O: Mag je deze antwoorden geven he? Misschien handig om erbij te hebben.

R1: Euhh, Bekwaamheid en de...

O: Je mag ook meekijken hoor, want ik heb hier

R1: Nee ik kijk even naar de definitie, we hebben deze natuurlijk wel doorgenomen, maar dat betekent niet dat ze allemaal helemaal meteen scherp in mijn hoofd zitten.

O: Nee

R1: Euhm... Ik zou zeggen vier, eens.

O: Oké, is de factor welwillendheid van toepassing op backlash from internal IT staf?

R1: Oh oké doen we het zo

O: ja dat is handiger denk ik

R1: Ja dat is handig zo. Euhm.. want het zijn..

O: even wachten, ik moet nog een toelichting bij de eerste, jij zegt bekwaamheid een vier

R1: O ok

O: Is eens?

R1: Ja.. Ik denk dat de bekwaamheid invloed kan hebben, überhaupt de bekwaamheid van medewerkers invloed heeft op het optreden van IT staf als een blokkerende factor. En dat je daarin ziet dat wat ik net zei euhm. juist de goede weglopen en de slechte blijven zitten. Dus waarmee je je totale bekwaamheid naar beneden gaat. Euhm, maar bekwaamheid ook de mate is waarmee ze mee euhm in staat blijven om hun werk op een goede manier uit te voeren.

O: Dus eigenlijk niet meer in staat zijn?

R1: Euh nee juist wel in staat zijn

O: Dus niet meer in staat zijn, als ze weglopen?

R1: Nee als ze een hoge bekwaamheid hebben, dan blijven ze ook in de situatie waarbij ze onzekerheid ervaren en veel gedoe, maar hierdoor beter in staat zijn om hun bekwaam hun werk uit te voeren.

O: Oke

O: Nu welwillendheid dan

R1: Ja euhm. die vind ik lastig moet ik zeggen, want het is euh... Is de welwillendheid van de leverancier een optelsom van de welwillendheid van de onderliggende IT medewerkers. Snap je dat?

O: ja

R1: Euhm, want vaak heb je in het...euhm. Er zit een bepaald koppelpunt in, op het moment dat heel veel mensen intern onwelwillend zijn dan krijg je daar last van binnen je IT staf, maar een individu die onwelwillend is en niet het standpunt van de organisatie inneemt heeft weinig invloed erop. Dus... euhm...even kijken hoor, die vind ik een moeilijke, want het kan ook zijn dat interne IT medewerkers ook nog je eigen medewerkers zijn, voor het moment dat je ze.

O: ja het zijn interne medewerkers.

R1: O ja dan ja. Dan heeft het niks meer te maken met de intentie van de leverancier, want het zijn je eigen mensen. Dus de leverancier is welwillend, maar je hebt nog je eigen mensen die je nog moet overdragen. Dus dan is het een factor die niet van invloed is op...

O: En is het dan niet van toepassing of ben je er dan geheel oneens ermee?

R1: Hij is niet van toepassing, want de leverancier zegt: ik ben welwillend om jou diensten over te nemen en er is een groep medewerkers die je nog moet overdragen, die hebben niks te maken met de welwillendheid van de leveranciers. Vat ik hem zo goed op?

O: Het is jouw antwoord. Ik ben het er mee eens.

R1: Euhm..Nu zit ik alleen even te denken of ik in deze lijn dan ook niet bekwaamheid op niet van toepassing moet.. Ja wacht even, ik ga toch twijfelen, sorry..

O: dat is goed, denk er maar over na

R1: Ik merkte met de overgang naar (NAAM ORGANISATIE) dat de welwillendheid van eigen medewerkers laag was en dat was daarmee ook een risico in je outsourcing, dus het heeft invloed op je vertrouwen.

O: Hoe heeft het dan invloed op je vertrouwen?

R1: Omdat je euhm..

O: Je vertrouwen richting je leverancier?

R1: Ja.

O: Maar hoe dan?

R1: Omdat je niet weet hoe ze zich zullen gaan gedragen. Op het moment dat ze nu al aangeven dat ze niet welwillend staan tegenover de leverancier waar zij straks voor moeten werken, schaadt dat het vertrouwen wat je dan op dat moment hebt in de leverancier. Maar het schaadt niet het vertrouwen van de welwillendheid van de leverancier, dat is het lastige hierin.

O: Het euh. Ik denk dat het mechanisme wat in werking treed ook los staan van de werkelijkheid Het

is de perceptie van de klant met betrekking tot de factoren.

R1: Ja

O: Maar als je denkt dat ik zie dit nu gebeuren binnen mijn organisatie, want als je een outsourcing traject met die betreffende klant niet in was gegaan dan was het niet gebeurt.

O: maar dan is je antwoord dus? We hebben het nog over welwillendheid wel?

R1: Ja, welwillendheid, dan wordt het toch een vier.

O: Nou die toelichting die luister ik wel terug.

R1: ja, euh. Integriteit gekoppeld aan de interne medewerkers. Poeh. Poeh. Ik zit weer te denken of deze dan niet van toepassing is. Ook hier zie je dat de integriteit van de leverancier anders is dan de integriteit van je eigen medewerkers, want die moet je nog overdragen.

O: ja, maar

R1: Als je het kan verduidelijken graag.

O: Het gaat erom dat bij backlash from internal IT staf, de medewerkers denken dat hun baan op de tocht staan .

R1: Ja

O: En daar zou de leverancier natuurlijk heel goed duidelijkheid over kunnen geven. En dat heeft wat mij betreft te maken met de integriteit van de leverancier.

R1: Ja

O: Eerlijkheid, betrouwbaarheid

R1: Ja ik zit even te kijken. Euhm. Ja want we hebben in het outsourcingtraject van zowel SSC-ICT als (NAAM ORGANISATIE) gemerkt dat er onzekerheid bestaat rondom het IT personeel, niet zozeer over de transitie, maar ook in de periode erna. Waarbij er bijvoorbeeld SSC-ICT toen zei: wij vullen nu een taakstelling in, jullie gaan schoon over. We vullen de taakstelling in bij de overgang, dus wij moeten nu uitspreken, terwijl de medewerkers daar heel onzeker over zijn, dat zij niet geraakt worden, want wij moeten zelf de taakstelling nog een keer uitvoeren voor hetgeen wat we al hebben. Dit gold ook bij (NAAM ORGANISATIE), dat ze daar de onzekerheid hadden over of (NAAM ORGANISATIE) niet na transitie met een schuif of reorganisatie erover heen ging komen, waarbij (NAAM ORGANISATIE) zei we doen het niet en prompt... deden ze het wel.

O: Dat heeft toch alles te maken met integriteit?

R1: Ja.

O: Kijk en dan kan ik me dus goed voorstellen dat als ...dat wij als klant zeggen, heh zo ga je niet met onze mensen om.

R1: Dus dan is het een factor die zeker van belang is, dus dan is het ook een vier.

O: Vier?

R1: Ja

O: We hebben ook nog vijf he?

R1: Ja dat weet ik, haha. Ik kom op vieren uit omdat als je weet dat je een outsourcing beslissing moet nemen, natuurlijk gaat je interne personeel dan zitten piepen. Op alle punten, maar je hebt eigenlijk de koers al ingezet, dus het gaat nooit je beslissing wel of niet outsourcen beïnvloeden.

O: Maar daar gaat het nu ook niet om he?

R1: Nee

O: Het gaat puur om het feit of die factor van toepassing is op het IT-outsourcing risico. Op dit risico. Je kunt denken een beetje, of helemaal niet of...

R1: Ook daarin zie je dat je best een denkslag moet maken wil je dat aan elkaar relateren.

O: Wacht even, nu hebben we deze vastgesteld en dan wil ik eigenlijk van jou horen, je hebt gezegd van nou voor bekwaamheid daarmee ben ik het eens dat die euhm.. zeg maar van toepassing is op backlash from internal IT staf. Euh maar, als je een rapportcijfer moet geven tussen 1 en 10 hoe veel zou bekwaamheid dan van invloed zijn op het geheel aan vertrouwen? Met betrekking tot dit IT risico.

R1: Kan ik elk cijfer maar 1 keer gebruiken?

O: Nee

R1: Kun je nog een keer de vraag herhalen?

O: Hoe groot of hoeveel invloed heeft bekwaamheid op het geheel aan vertrouwen met betrekking tot het risico backlash from internal IT staf? Zeg maar je bekwaamheid ga je verhogen, in hoeverre wordt dat dan doorberekend aan het totaal aan vertrouwen.

R1: Ja euhm.. ik vind het moeilijk om daar een cijfer aan te geven. Als ik de bekwaamheid verhoog dan.. euh.. een zeven denk ik

O: En waarom?

R1: Omdat ik denk dat euh.. je zegt dat .. euh.. uiteindelijk is bekwaamheid ook een soort van patroon dat je hebt. Op het moment dat je bekwaam bent en bekwaam handelt vanuit een professionele inslag euh.. dat kan je proberen te verhogen door het kennisniveau te verhogen, maar op het moment dat er andere factoren gaan spelen die sterker zijn, dan kan zelfs de meest bekwame persoon alsnog eh.. eigenlijk besluiten om niet dat professionele gedrag te vertonen.

O: En dat heeft weerslag op het vertrouwen?

R1: Ja

O: Oke, welwillendheid?

R1: Euh.. even kijken, de mate waarin je de welwillendheid

O: Invloed heeft op vertrouwen met betrekking tot het risico backlash from internal IT staf.

R1: Ik denk dat het een belangrijke relatie is. Ik denk dat het wel een negen is.

O: Waarom?

R1: Omdat als je dat euhm als je weet dat, dat goed zit, dan heb je het vertrouwen dat ook in een nieuwe situatie, een onzekere situatie mensen er toch van alles er aan zouden blijven doen om voor jou de IT in orde te houden, zeg maar. En euhm.. niet... en dat daar geen risico's optreden.

O: ja, je zegt net over de IT, maar je bedoelt de baanzekerheid voor de interne IT medewerkers?

R1: Ja maar ook het feit dat ze zich comfortabel gaan voelen in de nieuwe situatie, dat ze daar uitdagingen in zien en kansen in zien, dus dat ze eigenlijk de mate waarin zij echt bijna staan te wachten bij de voordeur staan te wachten totdat ze geoutsourcet gaan worden.

O: dan heb je het dus over de situatie dat waarin de medewerkers mee gaan, maar het kan natuurlijk ook zo zijn dat hun hele baan vervalt, maar goed dat is. Dat heeft niets te maken met welwillendheid alhoewel welwillendheid is in deze misschien ook wel van: kom maar je mag bij mij komen, met al je kennis.

R1: Ja en ehm. Wat hier bijvoorbeeld ook staat, intellectuele verlamming, productiviteitsverlies, stress en onzekerheid, weet je als je iets wil dan is dat een hele sterke driver om dat tegen te gaan.

O: Ja inderdaad, integriteit?

R1: Even kijken integriteit en de mate waarin integriteit van belangrijk is voor ... 8.

O: Waarom?

R1: Misschien wel een 9, omdat zodra het gevoel gaat ontstaan dat de leverancier niet betrouwbaar is, niet integer is, neemt het risico op backlash from internal IT staf enorm toe. Dat heb je eigenlijk ook gezien bij (NAAM ORGANISATIE). Ze vertrouwde (NAAM ORGANISATIE) voor geen meter.

O: Is de factor bekwaamheid van toepassing op contractual risk?

R1: Helemaal eens.

O: Waarom? En welk rapportcijfer

R1: Euhm... Eigenlijk is dat de grondslag voor het aangaan van je contract, of ze bekwaam zijn om het uit te voeren. En... ja kan ik dat zo stellen? Is dat überhaupt een risico?

O: Wat?

R1: De bekwaamheid om de taak uit te voeren?

O: Dat lijkt mij wel.

R1: Dus dan is het rapportcijfer.. Even nog een keer, Ja helemaal eens, het is een enorme factor en dan het rapportcijfer wat dat weegt.

O: Wat invloed heeft op het geheel van vertrouwen.

R1: Ja dat moet ik ook gewoon een tien geven. Welwillendheid is ook vijf, want uit welwillendheid spreekt ook bij mij de intentie, om even los van het contractuele juist, de dingen gewoon op te

lossen.

O: Los van het contractuele? Of naast het contractuele?

R1: Ja als het hier gaat om enigheid omtrent de details van een contract, op het moment dat je welwillend bent en je weet dat je er uit gaat komen met elkaar, weet je dan kan je bij wijze van spreken een two pager van het contract maken. Want dan weten we dat we niet alles hoeven vast te leggen, want dan weet je we gaan eruit komen, dus je hebt een samenwerkingsrelatie. Euhm.. dat is dus ook een enorme invloed op het contract risico, dus ook gewoon een tien. Gewoon maximale score.

O: Integriteit?

R1: Even kijken, dan is de vraag, in hoeverre is integriteit?

O: Is de factor van integriteit van toepassing op het risico contractueel risk?

R1: Ja vijf, ook, volledig. Maar ik denk dat de invloed kleiner is, omdat het niet hebben van integriteit in een contract, ja kijk dan kom je in een soort donkere wereld terecht. Dus.. Ja hij is uiteindelijk van enorme invloed, dat kan niet anders. Hij is heel erg van toepassing, maar de invloed is heel laag. Dus dan is het....

O: Waarom is het heel erg van toepassing dan?

R1: Ja nou wacht even... zeg ik het nou goed? Wat ik bedoel te zeggen is dat ..

O: Je moet open en eerlijk in een contract

R1: Als je niet eerlijk bent in een contract dan loop je een heel ander risico namelijk, dus.. euhm.. weet je je bent natuurlijk een totale idioot als je contractbreuk moet willig erin brengt en dit komt boven water, dan is dit zo evident en dan heb je een heel ander issue me elkaar. Dat de uiteindelijk invloed van integriteit niet zo groot zal zijn op het contractuele niveau. Zeg ik dat goed?

O: Nee dat laatste weet ik niet. Ik weet niet wat je bedoelt?

R1: Ja ik bedoel te zeggen, ik vind het belangrijk dat er integriteit ten aanzien van het contract zit, maar ik kan me niet indenken, dat het heeft.. namelijk niet heel veel invloed op mijn vertrouwensgevoel, omdat ik zelf de kans niet zo groot acht dat, dat daarin naar voren komt. Maar dat mag eigenlijk ook niet gezegd worden, want we hebben het helemaal niet over kans.

O: Maar stel dat het wel zou voorkomen?

R1: Ja als je kijkt naar kas maal impact, kans van slagen is heel groot dat iemand niet integer is in het afsluiten van een contract, dus.. euhm.. het is heel moeilijk. Het is een conceptuele worsteling waar je daarheen moet. Ja de factor integriteit is van toepassing op het risico van contractbreuk, de invloed van de relatie van integriteit op het totale geheel aan vertrouwen.

O: Kijk op het moment dat het zich voordoet, dat iemand binnen euh.. de contractuele risico's die er zijn niet integer is, is dat dan van veel of van weinig invloed op het totale vertrouwen?

R1: Ja veel, dan is het dus ook gewoon een tien. Alle vier de zaken zijn gewoon maximaal van toepassing.

O: Alle drie.

R1: Ja sorry, alle drie.

De factor bekwaamheid is vier van toepassing tussen de effectieve coördinatie tussen klant en IT-leverancier.

O: Waarom, wat is de toelichting?

R1: Omdat dit wat zachtere aspecten zijn, coördinatie aspecten zijn aan de voorkant wat minder hard te maken, dus euhm... Je denkt niet na over van is deze persoon met wie ik nu om tafel zit om op de lange termijn met mij te communiceren. Dit zit minder in je twijfel. Coördinatie kun je vrij gemakkelijk bereiken, of die effectief is komt voor een deel voort uit bekwaamheid, dus is iemand in staat om een nette mail te dichten, in staat om goede samenvattingen te sturen, goede rapportages, maar ik denk dat je uiteindelijk dat bekwaamheid of dat coördinatie op de andere aspecten veel groter is.

O: Even kijken, coördinatie aspecten zijn aan de voorkant minder hard te maken, bekwaamheid moet wel aanwezig zijn, maar zit minder in de scope, ofzo?

R1: Er zit minder een afbreuk risico op.

O: Aan de voorkant?

R1: Ja

O: Oke

R1: Dus de invloed van bekwaamheid op de effectieve coördinatie zou ik zeggen een ... even kijken.. de invloed van.. bekwaamheid van coördinatie op het totale geheel aan vertrouwen is een zes denk ik.

O: Waarom is dat een zes?

R1: Het heeft wat meer, coördinatie is een andere manier van... nogmaals coördinatie is wat minder hard, coördinatie elementen. Want coördinatie is eigenlijk gewoon de hele uitwisseling op dag tot dag basis met elkaar en daar speelt bekwaamheid echt wel minder een rol.

O: Oke, next.

R1: Dan vind ik welwillendheid in de coördinatie wel heel erg van belang.

O: Ja, een vijf? En waarom?

R1: Ja, omdat de welwillendheid bepaalt de effectiviteit ervan. Op het moment dat je niet welwillend bent dan komt de coördinatie niet van de grond en dan merk je dat je voortdurend tegen een blokkade loopt om dingen met elkaar uit te wisselen en met elkaar te communiceren.

O: Ja, oke.

R1: Dat betekent dat de invloed van welwillendheid daarmee ook grote is op het vertrouwen in de coördinatie. Ik denk dat het een 8 is. Nah ik zit nog even te denken aan het vorige, want bijvoorbeeld de projectleider die we hebben voor de uitrol van de nieuwe laptops is namelijk niet echt heel bekwaam, maar wel heel erg welwillend. Snap je? Dus.. ik merk dat de welwillendheid dan boven de bekwaamheid staat.

O: Ja eens.

R1: Aan de andere kant, onze relatiemanager is noch bekwaam, noch welwillend.

O: Daar hebben we dan ook niet zo veel vertrouwen in.

R1: Juist ja. Integriteit is ook heel belangrijk in de coördinatie.

O: Vijf?

R1: Vijf.

O: Waarom?

R1: Omdat het ook de basis is van de samenwerking, op het moment dat je in de coördinatie niet integer bent, dan stukt daarmee eigenlijk de coördinatie onderling, dan daalt de effectiviteit van de coördinatie naar nul, want je kan niet meer goed de dingen tegen elkaar afwegen of alles wel op een eerlijk en betrouwbare manier verloopt.

O: Ja.

R1: Dus de invloed van betrouwbaarheid op de coördinatie tussen klant en leverancier is een, en daarmee het vertrouwen is een negen.

De invloed van bekwaamheid op culturele verschillen tussen partijen. De factor bekwaamheid is van toepassing op culturele verschillen. Ik denk dat namelijk de essentie is van culturele verschillen, dat er een mismatch is tussen. Kijk jij bent in jouw cultuur bekwaam en ik ben in mijn cultuur bekwaam.

O: Ja zo.

R1: Snap je? In het geval van een offshoring traject wat in India als bekwaam wordt gezien, is compleet anders als wat bij ons als bekwaam wordt gezien.

O: Ja, maar heeft dat consequenties voor vertrouwen?

R1: Ja, ik vraag me af of er een correlatie is.

O: Dat weet ik ook niet. Het kan ook niet van toepassing zijn.

R1: Ja dat weet ik, maar dan moet ik hem wel goed formuleren. De factor bekwaamheid is ... , poeh wat moeilijk zeg. Is wel van invloed, een vier.

O: En waarom?

R1: Omdat je bekwaamheid wel meetbaar kan maken, dus je kan aangeven iedere helpdeskmedewerker uit India die moet een bepaald taalniveau hebben en die moet deze en deze cursussen hebben gevolgd. Dus je kan het beïnvloeden. Er is dus een relatie.

O: Rapportcijfer?

R1: Niet heel hoog, een zes.

O: En waarom niet zo hoog?

R1: Het .. euhm.... Op het moment dat je vanuit vertrouwen bekijkt heb je het idee dat je kan beïnvloeden. Je stelt gewoon de scholingsvereisten vast en daarmee heb je het vertrouwen dat er aan het culturele verschil voorbij gegaan kan worden.

O: Oke.

R1: De echte risico's zitten in de andere aspecten namelijk. Even kijken welwillendheid is.. ook van invloed met een eens.

O: Waarom?

R1: Ook daar weer ondanks dat je een andere achtergrond hebt of een cultuur verschil, op het moment dat je daar uitspreekt we willen proberen om het onderling te laten werken euhm.. maakt dat je rimpelingen glad kan gaan strijken. Dus ik vertaal dan ook de welwillendheid om over de eigen organisatie grenzen heen te kunnen kijken en daarmee te kijken wat er in een andere organisatie van belang gevonden kan worden.

O: Hoe bedoel je dat?

R1: Dat je als ik kijk naar bijvoorbeeld (NAAM ORGANISATIE) weet ik dat ze heel veel waarde hechten aan het financieel op orde zijn, omdat ze werken volgens een baten lasten systematiek en daarmee een control cultuur heerst. Op het moment dat ik daar welwillend tegenover sta, dan vind je elkaar makkelijker. Op het moment dat je het erkent dan.. Op het moment dat ze het richting ons zouden erkennen dat wij soms dingen met een Franse slag moeten doen omdat er een belangrijk operatie aan zit te komen en ze hebben daar wel begrip voor ondanks dat ze zelf niet zo zouden werken, dan merk je dat daar een soort begripsverhouding met elkaar gaat ontstaan. Dus de invloed van welwillendheid om over cultuur verschillen heen te komen, vertaal ik dan als verplaatsen in een ander, de invloed is daarmee een acht.

O: Ja.

R1: Integriteit, ook van belang, ook eens, omdat integriteit... euh.. even kijken... als het niet hebben van integriteit een uiting is van een bepaalde cultuur en daarmee dus het verschil ontstaat, dan is dat eigenlijk een totale, dat schoffelt de hele mogelijkheid tot samenwerking onderuit. Op het moment dat een cultuur bij voorbaat als niet integer wordt ervaren, dan is het vertrouwen in de samenwerking en het oplossen van de culturele verschillen onmogelijk, dus dan is de invloed ook een negen.

O: Bekwaamheid in difficulty in managing remote teams?

R1: Eens dat er een invloed is. Ik denk dat het een vijf is en ik denk omdat het gaat om een moeilijkheidsgraad, het is namelijk niet onmogelijk. Op het moment dat je bekwaam bent en ervaring hebt in het managen van teams op afstand, dat je hebt kunnen aantonen dat je dat op een goede manier hebt kunnen oplossen, dat dit het vertrouwen vergroot. Dus bewezen bekwaamheid daarin, om een bepaald probleem op te lossen. Ik waardeer die invloed met een acht, omdat de resultaten uit het verleden geen garantie geven voor de toekomst en dat je altijd weer vanuit je eigen belang redeneert.

Welwillendheid is van invloed op het managen van remote teams, eens, een vier. Namelijk de wil om de problematiek op te lossen. En de wil om daar structuren voor te bedenken om dat voor elkaar te krijgen, een zeven zou ik zeggen.

Integriteit , ik vraag me af of dit een relatie heeft met het managen van remote teams, ik zie daar niet een duidelijke relatie tussen of ik moet hem even missen. Nee, niet van toepassing.

O: Dan hoeft er ook geen rapport cijfer gegeven te worden.

R1: Dat is een breinbreker, die kan ik niet zien. Ja en nu kom je dus in een cirkel redenering, want dan krijg je dus lack of trust. Zeg ik het dan goed als ik zeg ja de factor bekwaamheid is zeer van invloed op het vertrouwen in de leverancier?

O: De lack of trust is dat dan he. Het gebrek aan vertrouwen.

R1: Oh ja, bekwaamheid is van invloed op het gebrek aan vertrouwen.

O: Bijvoorbeeld als er weinig bekwaamheid is..

R1: Ja dan is er geen vertrouwen.

O: Ja

R1: Ja maar dan kom ik dus. Eigenlijk is dit je hoofdconclusie. Als je niet bekwaam bent en niet integer en niet welwillend dan is er geen vertrouwen.

O: Ja als het goed is komt dat er uit.

R1: Ja bekwaamheid is van invloed en ja het is maximaal.

O: Tien? Allemaal Vijf Vijf?

R1: Ja allemaal maximaal, en tien tien.

O: Loss of control over data, bekwaamheid

R1: Ja, dat is een belangrijke.

O: Vier of vijf?

R1: Vijf, bekwaamheid. De invloed is een acht, je wil het idee hebben dat ze op een professionele manier in staat zijn om als een goed huisvader zorg te dragen voor jouw data en daar geen fouten in te maken, dus bewust bekwaam is dat dan. Weten wat ze aan het doen zijn met de gegevens waar jij heel veel waarde aan hecht.

O: Waarom geef je dat zo'n hoog rapportcijfer?

R1: Euhm.. omdat het vertrouwen zit in het met name, het gebrek aan vertrouwen zit hem in ze snappen het niet, ze zijn onbewust ervan of ze kunnen het niet.

O: Ja

R1: Snap je hem?

O: Ja helder. Welwillendheid?

R1: Welwillendheid vind ik wat meer.. welwillendheid is wel van invloed, een vier. Wil ik zorgen dat jouw data.. nee het is toch wel een vijf, dat zij aantonen dat zij het belang zien die jij hecht aan de data op dat moment. Dus euhmm.. En daar de invloed van welwillendheid is een acht, omdat je daar ook nog wel ziet, van oke, dat je basisafpraak, het gaat niet alleen om de welwillendheid, want je maakt daar ook gewoon afspraken over hoe daar mee omgegaan moet worden. Integriteit is van levensbelang op .. Als je het gevoel hebt dat ze niet integer met je data omgaan, dan kun je het net zo goed niet plaatsen. Dan weet je zeker dat je het verlies aan controle over de data gaat ervaren en dat je de data als het ware vogelvrij wordt verklaard. Dus een vijf en een tien.

R1: Opportunistisch gedrag, moet ik ze alle drie benoemen of mag ik het als één zien.

O: Als één.

R1: Oke. Bekwaamheid is van invloed op het opportunistisch gedrag, euhm een vier.

O: Waarom?

R1: Even goed proberen te zeggen. Ook dit zit weer een beetje in het onbewust onbekwaam. Op het moment dat je opportunistisch gedrag vertoont, op het moment dat je niet bekwaam bent tot wat je doet, dan kan dat juist leiden tot opportunistisch gedrag. Dus eigenlijk weet ik niet wat ik aan het doen ben, maar ik ben opportunistisch genoeg om me eruit te bluffen. Je zal dan.. je correleert dan bekwaamheid aan in principe niet opportunistisch, want je weet wat je aan het doen bent. Dus of je slaat door, je weet zo goed wat je aan het doen bent, dat je daarmee juist opportunistisch aan het worden bent.

O: Dus bewust opportunistisch?

R1: ja.

O: Gehaaid?

R1: Ja, want je hebt al zoveel van dit soort contracten gehad, je weet exact waar de marges zitten, je weet exact hoe je moet inbieden en weet exact hoe je alles moet plooiën om voor jezelf het maximale eruit te halen. Dus zowel het niet bekwaam zijn als het over bekwaam zijn zou kunnen leiden dat opportunistisch gedrag.

O: En de invloed die het heeft op het geheel aan vertrouwen?

R1: Ik denk dat de invloed niet zo heel groot is omdat je het vaak niet verwacht. Het is geen factor die heel duidelijk, nah ja ik denk er wel eens over na, weten ze nou heel donders goed waar ze mee

bezig zijn om het optimale eruit te halen. Maar dan raakt je eigenlijk meer de integriteit ervan, dan ben je de boel aan het verzieken.

O: Ja, dus...

R1: Bekwaamheid, een zeven. Het moet wel kunnen, of totaal niet kunnen en beiden leiden tot opportunistisch gedrag.

O: Welwillendheid?

R1: Vijf, ik denk op het moment dat je welwillend bent in een relatie dat je zal beslissen geen opportunistisch gedrag te vertonen. Het zijn bijna twee tegenovergestelde dingen van elkaar.

O: Dus dan heeft hij ook een hoge invloed?

R1: Ja. Een negen. Vaak leg je daarmee de welwillendheid alleen nog maat uit in je eigen voordeel. Snap je wat ik daarmee bedoel? Het voorbeeld wat hier wordt gegeven; vergelijk het met de loodgieter die komt met extra kosten op het moment dat de watertoevoer al is stilgelegd. Partners die deze benadering gebruiken proberen in de contractuele fase dingen open te laten. Het lijkt alsof ze heel welwillend zijn, maar feitelijk maken ze gewoon totale misbruik van de situatie. Echte welwillendheid leidt niet tot opportunistisch gedrag.

Integriteit, ook een vijf. En ja dan kom je echt in de fraudeachtige modellen. Ik ben nu doelbewust vanuit mijn onbetrouwbaarheid aan het zorgen om maximale uit het contract te slepen en je pakt eigenlijk alles aan om voor mij gunstig gedrag in te brengen. Je hebt het dan in feite in alle kanten ingebouwd in de relatie, dus de invloed van integriteit op opportunistisch gedrag of het risico van opportunistisch gedrag is een negen.

Beveiliging en privacy. Bekwaam is een invloed, ben jij überhaupt in staat om te zorgen voor een afdoende beveiliging. Dus dat is een hele grote correlatie, dus een vijf en de invloed van die bekwaamheid is ook heel hoog, dus een 10 zou ik zeggen.

Welwillendheid heeft ook een duidelijke relatie en is zeker van invloed, daarmee een vijf.

Welwillendheid bepaalt namelijk de mate waarin jij het risico wat de klant ervaart ook daadwerkelijk serieus neemt. Dus hij is wat minder sterk dan de bekwaamheid.

O: Qua invloed bedoel je?

R1: Ja qua invloed, omdat je toch al daar weer zit, we hebben kaders, we hebben afspraken, we hebben regels om met dingen om te gaan. Daarmee is de invloed van welwillendheid daarmee ietsje zwakker, maar nog steeds wel hoog.

O: Ja en je hebt natuurlijk vanuit de welwillendheid kan er wel zijn, maar ook de leverancier heeft zich binnen bepaalde kaders te bewegen.

R1: Ja, ja, tenzij het laatste, indien ze niet integer zijn dan stort eigenlijk alles daarmee als een kaartenhuis in elkaar.

O: Dus volgens mij zitten we alle drie op vijf, waarbij bekwaamheid zit op een tien, welwillendheid op een acht, en integriteit op een tien.

R1: Ik zit wel de hele tijd aan de hoge kant, want ik denk dat als het van toepassing is dan is de invloed ook hoog.

O: Ik weet niet of je het moet zien als een onvoldoende, iets kan ook gewoon.. kijk als je kijkt van dit is het uiterste en dit is het andere uiterste, dat je ergens daar (onderzoeker wijst een punt aan op tafel) zit van invloed. Sommige dingen hebben niet zo heel veel invloed op het totaal aan ... Maar goed dit is jouw interpretatie.

R1: Ja dat klopt. Even kijken dan komen we op het volgende. Single / double moral hazard, dan hebben we die weer. De factor van bekwaamheid heeft wel een relatie met single / double moral hazard.

O: Waarom?

R1: De bekwaamheid om überhaupt tot informatie uitwisseling te komen namelijk.

O: Ik weet niet of je hem zo moet int...

R1: Nee sorry je hebt gelijk.

O: Het gaat meer om.. ik vind dit zelf ook een van de lastigste, je moet meer kijken naar moreel wangedrag. Ik denk dat je dat zo zou moeten bekijken en heeft bekwaamheid daar dan iets mee te

maken?

R1: Ja dat vind ik wel een lastige ja. Ik denk het niet eigenlijk, omdat als je moreel wangedrag vertoont, hoe bekwaam je ook bent, je neemt op dat moment gewoon een andere beslissing.

O: Ja.

R1: Zodra je het on intentioneel doet dan heeft het niks meer te maken met je moraliteit te maken. Dus er is geen relatie denk ik.

O: Met welwillendheid?

R1: Welwillendheid heeft wel invloed. Is wel een factor voor moral hazard, dat bepaalt namelijk de factor waarin jij besluit.

O: Vier of vijf? Of drie? Neutraal kan ook.

R1: Neutraal zegt me niet zo veel.

O: Neutraal zit er tussen in natuurlijk, beetje wel en een beetje niet.

R1: De factor welwillendheid heeft.... . Op het moment dat je welwillend bent naar een andere partij zou je niet geneigd zijn om moreel wangedrag te vertonen. Of is het welwillendheid... nee.. nee. Ik vind dit een lastige om uit te leggen.

O: Ja? Vier?

R1: Ja een vier.

O: en de invloed?

R1: Als je zegt moreel wangedrag, dan is dat altijd een keuze, op het moment dat je welwillend bent dan maak je niet de keuze tot amoreel gedrag.

O: Ja, ja, in deze hangt welwillendheid en integriteit misschien wel heel dicht tegen elkaar.

R1: Ja als je niet integer bent dan ben je bijna per definitie amoreel. Dat is een euh..

O: Dus die zit vijf?

R1: Ja.

O: Maar dan de rapportcijfers? Hoeveel heeft welwillendheid dan van invloed op het totaal aan vertrouwen?

R1: Een acht.. nee een zeven denk ik.

O: En integriteit?

R1: Ja hoog, dat is dan ook een negen of een tien. Nou moet ik kiezen he? Doe maar een tien. Even kijken de factor...

O: Bekwaamheid

R1: Bekwaamheid

O: op goal incongruence

R1: Ik denk dat er geen invloed is.. of neutraal. Ik zie niet waar de bekwaamheid van een medewerker, echt de bekwaamheid, een doelstelling van een werknemer dat, dat leidt tot een andere doelstelling van de organisatie.

O: Is dat dan niet van toepassing of ben je het niet eens met de stelling? Of neutraal? Ja dat kan ook hoor.

R1: Voor mij maakt het niet uit, er kan best een relatie zijn, maar voor mij is hij neutraal.

O: oke en een rapportcijfer?

R1: Nou zit ik even te denken, als jij als medewerker niet bekwaam bent, leidt dit dan dat je op een andere doelstelling zit als het bedrijf, volgens mij niet. Dus dan is het een neutrale, dus de invloed van bekwaamheid op het risico...

O: Op het totale vertrouwen is dan? 1,2,3?

R1: Euhm.. een drie

O: Welwillendheid?

R1: Welwillendheid is wel van belang.

O: Vier of vijf?

R1: Dat is een vier, want dat bepaalt in hoeverre de medewerker zich ook daadwerkelijk achter de doelstellingen van de organisatie zich zal scharen. Want het gaat weer om de werknemer.

O: Nou de leverancier is welwillend.

R1: De leverancier is welwillend, maar er bestaat wellicht een risico dat de leverancier als organisatie wel welwillend is..

O: Maar het gaat erom of de leverancier hier rekening houdt met de werknemers doelstellingen van de klant.

R1: O ok, mijn werknemers, ik dacht de werknemers van de leverancier.

O: Nee.

R1: Oke, nee ik zat naar hun.. euh.. Dan is het bij de vorige gewoon geen relatie. .

O: Dan is het geheel oneens, zal ik hem dan ook op 1 zetten?

R1: Of niet van toepassing. Ja dat vind ik..

O: of 0?

R1: Eigenlijk is mijn mening dat hij niet van toepassing is.

O: Wat? De invloed?

R1: Ja, maar dan is het alsnog mijn mening. Misschien moet je al mijn niet van toepassingen als geheel oneens beschouwen. Ik wil niet jouw methode onderuit halen.

O: Ah ja zo. Inderdaad en dan als niet van toepassing bij de invloed zetten. Misschien moet ik niet van toepassing ook weghalen als antwoord mogelijkheid.

Notitie onderzoeker: de antwoordmogelijkheid, niet van toepassing, wordt geschrapt.

O: Even kijken de welwillendheid

R1: De welwillendheid is wel van invloed

O: Ik had een vier, maar moet nog het rapportcijfer.

R1: Euhm.. Het idee van de leverancier verplaatst zich achter.. even kijken hoor... ik moet hem weer goed vertalen.. is de welwillendheid van de leverancier richting jouw al organisatie van invloed op het feit dat....

O: Dat de leverancier zelf rekening houdt met de werknemersdoelstellingen, zeg maar.

R1: Ja maar gaat het over mijn bedrijfsdoelstellingen en mijn werknemersdoelstellingen op een lijn zitten.

O: Ja, maar als de leverancier moet daar ook bij aansluiten. Dat die rekening houdt met de persoonlijke doelstellingen van de werknemers.

R1: Of met mijn bedrijfsdoelstellingen?

O: Als het goed is gaat die leverancier werken aan jouw bedrijfsdoelstellingen, toch?

R1: Ja

O: Dat gaat die doen, maar daarin moet hij dus niet vergeten de persoonlijke doelstellingen van de medewerkers mee te nemen.

R1: Maar dat kan hij niet doen, want ik heb een andere relatie met mijn leverancier. Dat is ook weer een interne problematiek

O: Dat weet ik niet.

R1: Ik zeg als bedrijf we; weg gaan met zijn alle rechtsaf. Bij mij willen dan heel veel medewerkers linksaf, ik wil dan niet dat mijn leverancier rekening gaat houden met de persoonlijke doelstellingen van de medewerkers die een andere kant op willen lopen.

O: Nee, maar hij moet wel meegaan met het feit dat jij ook wil dat die persoonlijke doelstellingen van die medewerkers linksaf gaan. Moet hij niet denken, nee dan ga ik toch rechtsaf.

R1: Nou dan gaan we het wel heel oprekken. Weet je wel zeker dat het niet zijn werknemers zijn, maar mijn werknemers.

O: Ja

R1: Indien de leverancier geen rekening houdt met de persoonlijke doelstellingen van de medewerkers van de klant is, het resultaat informatie-asymmetrie tussen klant en leverancier. Ja dan is welwillendheid wel een factor. Dus een vier zou ik zeggen. De invloed hecht ik niet heel zwaar aan, een zeven. Nah dat is niet waar.. een acht.

O: Waarom?

R1: Omdat uiteindelijk de leverancier de medewerkers wel op een juiste manier moet bedienen

zodat zij ook de doelstellingen moeten kunnen behalen.

O: Integriteit op goal incongruence?

R1: Op het moment dat de leverancier niet betrouwbaar is, is dat dan van invloed op het hebben van...

O: Het geen rekening houden met de werknemersdoelstellingen.

R1: Dit vind ik ook een lastige. Ik zie daar ook geen hele duidelijke correlatie tussen.

O: Een of twee?

R1: Euh.. Twee.

O: En dan de invloed?

R1: Een vier denk ik.

O: Waarom?

R1: Ja kijk, op het moment dat je niet doet wat je zegt, ja natuurlijk blijft er dan wel een verschil staan en treedt natuurlijk op dat persoonlijke doelstellingen niet worden gehaald. Je bent niet aan het leveren conform afspraken.

Euhmm.. supplier employees have poor communication skills. Nee hier speelt wel de factor bekwaamheid een rol. Communiceren is een vak zullen we maar zeggen. Zijn ze in staat om op een juiste manier gesprekken te voeren met de klant, dus een vier zou ik zeggen. Geen vijf omdat ze er uiteindelijk toch wel uitkomen. Het is wel van invloed op het vertrouwen, dus ik zou zeggen een acht.

O: Waarom?

R1: Heb ik dat net niet al gezegd?

O: Ja, heeft invloed op vertrouwen.

R1: Omdat je zeker wil weten dat je medewerkers op een adequate manier geholpen worden.

O: Ja en indien dat niet gebeurt dan zal dat.. effect hebben.

R1: Ja als je ziet dat ze niet in staat zijn om op een goede manier te communiceren over zaken dan heeft dat invloed op je vertrouwen.

O: Grote invloed dus?

R1: Ja, nou misschien een zeven. Het is een soft skill en dat is makkelijk te verbeteren.

O: Welwillendheid?

R1: Welwillendheid heeft ook invloed. Is in ieder geval ook een factor. Wil de medewerker van de leverancier überhaupt een fatsoenlijke communicatie voeren met de klant.

O: Vier of vijf?

R1: Ja uiteindelijk ga je er hier ook vanuit dat er een sturingsstructuur bestaat. Je kan moeilijk als medewerker van een leverancier weigeren om überhaupt met de klant in contact te treden, dat daar wel een sturingsmechanisme optreedt, dus ik zou zeggen een zeven ook.

O: Maar is het een vier of een vijf?

R1: Een vier, sorry. Met een invloed van een zeven. En dan integriteit... vind ik ook een lastige uiteindelijk. Ik zie geen duidelijke correlatie tussen integer zijn en over goede communicatieve vaardigheden beschikken.

O: Één?

R1: Ja. Het zal natuurlijk nog wel van invloed zijn op het moment dat je gaat liegen tegen klanten, maar dat zijn dan incidenten.

Einde interview

11.8.2 Respondent 2

1. Formele vragen bij start van het interview

Opmerking: dit is een gestandaardiseerde tekst en geen letterlijke transcriptie. De onderzoeker leest onderstaande vragen voor:

- Dit gesprek wordt opgenomen, geeft u hier toestemming voor?
- Deelname van dit onderzoek is vrijwillig en indien u wilt stoppen kunt u dit te allen tijde aangeven. Stemt u toe om mee te werken aan dit onderzoek?
- De resultaten van dit interview worden anoniem verwerkt in een openbaar eindverslag. Geeft u toestemming om het resultaat van dit interview te verwerken in een openbaar eindverslag?

2. Introductie onderzoek

Hier wordt door de onderzoeker het onderzoek uitgelegd. Niet getranscribeerd.

3. Begrippen doornemen

De begrippen zoals deze zijn toegestuurd voor aanvang van het onderzoek worden met de respondent besproken. Aan de hand hiervan stelt de onderzoeker vast dat de begrippen overeenkomen met de visie van de respondent over deze begrippen. Niet getranscribeerd.

4. gegevensverzameling

De wijze van vragen stellen en te geven antwoorden worden met de respondent besproken en de onderzoeker geeft een voorbeeld van een vraag/antwoord. Niet getranscribeerd.

Vanaf het moment dat de vragen met betrekking tot de relatie tussen de factoren van trustworthiness en de ITO-risico's worden gesteld is het letterlijk getranscribeerd.

O: Is onderzoeker

R2: Is respondent 2

O: is de factor bekwaamheid van toepassing op het risico backlash from internal IT staf?

R2: Gaat dit dan over mijn eigen mensen?

O: Nee, het gaat erom of je daadwerkelijk de relatie ziet.

R2: Ja, maar welke mensen, welke internal IT staf? Die van de eigen mensen? Of van de leverancier?

O: O zo, ja, van de eigen mensen.

R2: Dat hangt niet perse af van het vertrouwen wat ik in de leverancier heb af of mijn mensen....

O: De bekwaamheid van de leverancier, zo moet je het dan zien.

R2: Het hangt meer af van of de leverancier concurrerende dienstverlening doet, maar als ik een leverancier uitnodig, maar die doet totaal iets anders dan mijn mensen. Ik denk niet dat daar een relatie moet zijn.

O: Die backlash wordt ook meer uitgelegd van er komt een moment.. je gaat outsourcen, je hebt eigen IT mensen, nou die IT mensen kijken daar natuurlijk sceptisch tegen aan, want die denken mijn baan staat straks op de tocht. Ik zou mijn baan kunnen verliezen of ze gaan over naar de IT leverancier, wat bij ons het geval is geweest.

R2: Dan hoort bij de vraag dat ik ga outsourcen, dus dan ga ik hetzelfde werk wat wij doen ook uitbesteden.

O: Ja het is allemaal binnen de outsourcing context. Alle risico's, die komen vanuit outsourcing.

R2: Oke.. ja dan hangt het van de mensen af, maar ja

O: Dan is het dus de vraag of er dan een relatie is met dit risico met bekwaamheid van de leverancier, daar hebben we het over. Want het vertrouwen in de leverancier bestaat dus uit drie componenten, bekwaamheid van de leverancier, welwillendheid van de leverancier en de integriteit.

En je hebt vijf keuzes, als je denkt ik zie daar helemaal geen relatie, dan ben je het er geheel oneens mee, het kan zijn dat je denkt; het kan zijn dat er een relatie is, maar ik zie het niet dan zou je neutraal kunnen doen.

R2: Ik denk we dat er een relatie is, ik zou dus zeggen eens, nummertje vier.

Maar er hoort natuurlijk ook een verhaaltje bij. Waarbij je kan checken of ik de vragen ook begrijp. Maar we gaan dus iets outsourcen dat betekent dat het werk wat wij doen ook aan derden uitbesteden, misschien omdat wij te veel hebben of de mensen niet hebben. Of onze mensen daar last van hebben in die zin dat ze gaan tegenwerken dat hangt ervan af wat de situatie is. Gaat het ten kosten van de eigen banen of gaat het een verlichting opleveren van de werkdruk. In het eerste geval als het ten kosten gaat van mogelijke banen bij intern dan ga je zeker tegenwerking krijgen en een paar haantjes de voorste, maar als het niet ten kosten gaat van eigen banen, maar het zou de werkdruk tegenhouden, dan verwacht ik wel meer medewerking.

O: Is dan de relatie met bekwaamheid?

R2: Dan is er dus geen relatie met trust in de leverancier. Dus ik denk dat de relatie er dus niet echt ... het hangt niet van dit factor af. Is outsourcen per definitie dat je ook je eigen taken uitgeeft.

O: Nee dat hoeft niet, je kunt op verschillende manieren outsourcen, natuurlijk. Je kunt...

R2: Nee maar dat je dan ook minder mensen..., of dat je mensen gaat ontslaan.

O: Ook dat hoeft niet. Je kunt heel extreem outsourcen, maar als je kijkt in ons geval, zin de mensen ook daadwerkelijk allemaal over gegaan.

R2: Ja, oke. Dat kan ook nog tegenwerken. De mate van tegenwerken hangt dus meer af van wat voor een consequenties het heeft voor de medewerkers, dan of we vertrouwen hebben in de partij. Maar dat heeft ook wel, dus als mensen uiteindelijk tevreden zijn en akkoord zijn met het feit dat ze mee gaan naar een derde partij dan willen ze dat het natuurlijk wel een geode partij is, dat ze daar kunnen groeien. Dus als ze vertrouwen hebben in de partij zullen ze veel minder tegenwerken en wellicht zelfs meewerken. Dus zo gezien zie ik die relatie.

O: Oke, maar nu pak je vertrouwen heel breed, even terug gaan op de drie... heeft het dan te maken integriteit, welwillendheid of bekwaamheid?

R2: Euhmm.. Ja

O: Ik hoor je eerst zeggen bekwaamheid daar

R2: Ik vind het lastig..

O: Het is ook lastig

R2: Ik denk dat bekwaamheid heel belangrijk is, over het algemeenheid van de situatie van oke als mensen bijvoorbeeld over gaan naar de leverancier, wat ook een vorm van outsourcen is dan zullen ze de bekwaamheid, welwillendheid en integriteit van de leverancier wel belangrijk vinden, maar zeker de bekwaamheid. Ik schets nu een speciale situatie van outsourcing.

O: Ja dat de interne medewerkers het wel belangrijk vinden dat de nieuwe IT-leverancier bekwaam is, zo?

R2: Als onze eigen mensen naar die leverancier over moeten dan is natuurlijk wat zij van die leverancier vinden erg belangrijk. Of ze mee werken of tegen werken.

O: in deze specifieke situatie is dat dus wel belangrijk, dus dan zeg je eigenlijk dat er een relatie bestaat.

R2: Ja.

O: Alleen in de ene situatie zal het wel zijn en in de andere situatie niet.

R2: Ja.

O: Dus je zei eens he? Dat zei je eigenlijk al.

R2: Ja er is altijd wel een relatie.

O: Ok.

R2: Ook als natuurlijk hun werk wordt overgenomen en ze worden ontslagen dan is er natuurlijk ook een relatie. Maar dan is de situatie toch heel anders, dan boeit het ze eigenlijk niet wat voor soort organisatie het is, of ze wel of niet gaan tegenwerken.

O: Ja. Oké, dan is er een relatie en dan zou ik graag een rapportcijfer willen van 1 tot en met 10 hoe sterk de relatie van invloed is op het geheel aan vertrouwen.

Je hebt die drie punten, die zullen het totaal aan vertrouwen geven, maar als je alleen de relatie van de factor bekwaamheid bekijkt, hoe hoog zou hij dan scoren?

R2: Een relatie tussen bekwaamheid en vertrouwen?

O: Je hebt gezegd dat er een relatie is tussen bekwaamheid en backlash from internal IT staf, dat is het risico. Hoe groot zal de relatie op het geheel aan vertrouwen zijn?

R2: Ik vind eigenlijk de situatie nog te vaag om de relatie te kunnen duiden. Dus het hangt een beetje af van hoe je outsourcet.

O: Volgens mij zij je net dat inderdaad dat het risico zich daadwerkelijk voordoet en de relatie doet zich voor dan is het wel van belang, hoe groot is het dan van belang. Want het kan namelijk ook zo zijn dat het helemaal niet voor doet en dan is de invloed ook niet van belang.

R2: Ik zit even te kijken.. Ik denk van een schaal van een tot tien en dan de mate van.. ja een zeven denk ik.

O: Kun je uitleggen waarom het een zeven is?

R2: Ja ik denk hetzelfde verhaaltje als daarnet, als mensen naar een andere organisatie toe moeten vinden ze het wel fijn als het een goede organisatie is.

Dus als dat niet zo is dan gaan ze wel piepen, gaan ze sowieso wel. Als het een goede organisatie is da... ja dus het heeft zeker wel invloed.

O: Ja, oke. Euhmm. De welwillendheid. Is de factor van welwillendheid van toepassing op backlash from internal IT staf?

R2: ja die is hetzelfde als... die drie factoren.. het is allemaal vertrouwen en die bestaat uit drie factoren en ze zullen allemaal wel invloed hebben.. Maar dan denk ik aan die... welwillendheid ook een zeven. Als ze wel bekwaam zijn, maar niet willen dan vind ik dat ook niet fijn.

O: En is dat dan ook een vier, eens of geheel eens?

R2: Ja ook een vier, eens. Ik ben nooit zo uitgesproken, het zal meestal wel een twee, drie of een vier worden.

O: Dat is prima. En integriteit ook een vier dan?

R2: Ja en ook een zeven. Misschien ability dan een acht, ik denk dat dat wel iets meer is dan de andere.

O: Oke, even kijken. Gaan we naar bekwaamheid op contractual risk. Dus de problemen die zich voordoen met betrekking tot contracten. Is bekwaamheid dan van toepassing op contractual risk?

R2: En de mate van vertrouwen? Het gaat erom of je vertrouwen hebt in de partij.

O: Ja en dan specifiek. Het vertrouwen is het hele plaatje van bekwaamheid, welwillendheid en integriteit en eigenlijk moet je het uit elkaar trekken. Heb je.. als je kijkt naar die leverancier, is bekwaamheid dan van toepassing op het risico met betrekking tot contracten?

R2: Ja, dat hoort er wel bij vind ik.

O: is het dan een vier of een vijf?

R2: Een vier

O: Waarom vind je dat het erbij hoort?

R2: Je kan op dat punt natuurlijk, als je uit gaat van vertrouwen, dan loop je daar risico. Trust loop je altijd een risico.

O: Maar specifiek qua bekwaamheid dan.

R2: Ja dan loop je ja, nou als de organisatie uiteindelijk niet zo bekwaam lijkt te zijn. Wat in het contract staat klopt ook niet echt.

Nou ja het bedrijf zelf loopt ook een risico natuurlijk, als ze niet waar kan maken, dan ben ik ze niet verplicht om te betalen, maar uiteindelijk loop je gewoon risico op van alles en nog wat. Dus nee

O: En de invloed dan, daarvan? Beïnvloed bekwaamheid m.b.t. contractuele risico's op het geheel aan vertrouwen?

R2: Ja een acht.

O: Waarom is dat een acht?

R2: Ja ik denk dat het gewoon. Je kan de mist in gaan als het contract niet goed in elkaar steekt.

R2: Uiteindelijk de contracten bij ons... nee ja dat kan, zeker bij nieuwe contracten.

O: Welwillendheid bij contractuele risico's?

R2: Ja stel dat ze dus uiteindelijk minder welwillend blijken, maar wel bekwaam en integer wat is dan het effect. Ik denk dat dan het risico minder is.

O: Er is dus wel een relatie maar de invloed is minder, bedoel je dat?

R2: Ja..

O: Een vier?

R2: ja en een zes ofzo. Bijna neutraal ofzo.. ja dat is goed.

O: Ja? En integriteit?

R2: Ja daar loop je dan wel weer risico, als ze op dit punt niet eerlijk blijken te zijn dan ja.

O: Dus er is een relatie? De relatie is dan eens of geheel eens.

R2: Ja een vier.

O: Eens dus en de invloed?

R2: Een zeven.

O: Nog onder bekwaamheid dan? Want voor bekwaamheid heb je een acht.

R2: ja

O: Oke, de factor bekwaamheid is die van toepassing op coordination between client en supplier?

R2: Ja hier loop je natuurlijk ook risico. Het is sowieso wel eens dat er een relatie bestaat.

O: Waarom? Hoe zie jij dat?

R2: Bij ability denk ik dat er minder is. Dus dan is... weet je, je schat in dat je een goede relatie onderhoudt en coordinatie is daar een belangrijk onderdeel van, zoals het hier genoemd wordt. Maar ik vind dat meer een relationeel aspect en dat vind ik minder bij ability en bekwaamheid horen. Maar daarom denk ik dat bekwaamheid daar minder invloed op heeft.

O: Dat er dus wel een relatie is of dat er zelfs geen relatie is, dat kan natuurlijk ook?

R2: Doe maar neutraal.

O: Oke dan de invloed?

R2: Neutraal is dan toch geen invloed toch?

O: Nou ja dat weet ik niet, dat weet ik niet, dat hoeft niet.

R2: Vijf, zes, wat is dan neutraal?

O: Een vijf denk ik.

R2: Doe maar een vijf. De welwillendheid vind ik dan weer wel belangrijk en als dat uiteindelijk niet zo blijkt te zijn denk ik dat je ook een slechte coördinatie hebt. Dus ik zou zeggen eens en dan een negen ofzo.

O: Integriteit?

R2: Ik denk dat als die uiteindelijk minder blijkt te zijn dat je coördinatie dan ook niet lekker loopt. Dus ook eens en een negen of een acht. Doe maar een acht.

O: Oke, dan hebben we bekwaamheid en cultural differences between client and supplier.

R2: Ook hier kan je natuurlijk risico lopen en heeft wat mij betreft ook veel minder met ability te maken. Dan voor ability en cultural difference geen relatie

O: Ability and cultural differences geen relatie?

R2: Nee

O: Dus geheel oneens, of?

R2: Ja doe dat maar.

O: dan is er geen relatie en geen invloed.

R2: Ja dat geldt eigenlijk dan ook voor die coordination, doe dan maar een 2, kan dat nog?

O: Bij de coordination terug? Ja hoor dat is goed. En dan de invloed, daar heb je een vijf de vorige

R2: Ja dan ook een vijf

O: Als je echt geheel oneens bent dan is er geen invloed, dan ben je volledig oneens met de relatie en is er geen invloed. Bij neutraal zie je nog iets en bij oneens zou er nog een opening kunnen zijn, maar om nog even terug te gaan op coordination between client and supplier heb je bij ability

gezegd een 2 nu, dat heb ik verandert, maar voor invloed stond er een vijf, moet die ook naar beneden bijgesteld worden?

R2: Ja doe dan ook maar een drie.

O: Oke

R2: Cultural differences bij ability wordt dan een 1.

O: Ja die heb ik en dan is er helemaal geen invloed.

R2: Bij welwillendheid, ja daar loop je dan wel risico, eens en een acht of zo.

O: En waarom?

R2: Nou ja ik denk dat als je.. bij welwillendheid hoort dat je elkaar accepteert en dat gaat wel wat verder dan.. dat gaat net zo ver als wie je bent en wat je cultuur is.

O: Waarom schat je de invloed daarvan zo hoog in?

R2: Nou ja omdat welwillendheid te maken heeft met ...

O: Hoe meer welwillend mensen eigenlijk zijn, de leverancier eigenlijk is hoe meer vertrouwen je hebt dat het wel goed komt tussen de culturele verschillen?

R2: Ja dat is niet iets wat je van te voren op papier kan afspreken, van we gaan 's middags thee drinken.

O: Integriteit?

R2: Ja die is hier ook van belang, alleen iets minder. Dus eens en een acht of zo.

O: En waarom? Je zegt wel minder, maar je scoort hem hetzelfde.

R2: Ja dus dat klopt niet. Ik dacht misschien de welwillendheid geheel eens en dan hoort daar een negen bij ofzo. En integriteit zou ik zeggen een eens en een zeven.

O: Waarom? M.b.t. integriteit?

R2: Nou ik denk dat als je welwillend bent dat, dat de grootste invloed heeft en als je iets minder integer blijkt te zijn, dat hoeft niet perse slecht te zijn. Als je om een goede reden... dus maar uiteindelijk kan dat wel zijn effect hebben, maar ik denk gewoon minder.

O: Bekwaamheid is die van toepassing op managing remote teams?

R2: Ja daar loop je denk ik een risico bij ability, dus als ik de partij vertrouw op zijn vaardigheden, maar uiteindelijk toch minder blijkt te zijn, daar zie ik wel een risico, zeker bij teams die verder weg blijken te staan. Dus eens en een zeven. Ja welwillendheid eigenlijk hetzelfde en integriteit ook.

R2: Lack of trust, Volgens mij is de vraag of dat een onderdeel is van de drie. Ja dat is zeker.

O: een vijf dan?

R2: Ja een vijf. Dus als ik geen vertrouwen heb in een partij.. Ja ability heeft zeker.. ja.. daar loop je risico. Lack of trust.. ja..

O: En de invloed daarvan?

R2: Ja dat is dan een acht.

O: Waarom?

R2: Nah ja als blijkt dat ze niet zo bekwaam zijn dan heb ik wel minder vertrouwen in de partij, in wat ze kunnen.

O: Ja

R2: Uiteindelijk.

O: En welwillendheid?

R2: Eigenlijk hetzelfde. Nah ja.. een zeven

O: En ook een vijf? Geheel eens?

R2: Ja

O: En integriteit?

R2: Een vier en dan een zeven.

O: Waarom is dat een zeven?

R2: Iets meer dan gemiddeld.

O: Omdat die minder zwaar weegt op het geheel aan vertrouwen?

R2: Ja ik denk dat die ook veel minder vaak ook echt voorkomt, ik zie dat.. ja ik heb daar wat minder mee met integriteit. Dat zit over het algemeen... nah dat is niet waar.. ja.. is voor mij gewoon een mindere factor van belang.

O: Oke, bekwaamheid op loss of control over data?

R2: Ik denk dat ik daar niet zo heel veel relatie zie, dat zijn hele concrete afspraken die je daar kunt maken. En dan moet je wel heel erg onbekwaam zijn om die te omzeilen, dus ik denk dat die relatie vrij minimaal is, dus dat ik.. op basis van mijn vertrouwen die ik heb in mijn leverancier, denk ik niet dat, stel dat mijn vertrouwen onterecht is, dat dat heel veel impact heeft op het verlies van data.

O: Dus de bekwaamheid van de leverancier heeft geen invloed op het verlies van data.

R2: Nah ja, ik denk dat.. iets. Is neutraal ook iets of is dat nul?

O: Neutraal is wel iets ja.

R2: Oke, doe dan maar neutraal.

O: En de invloed?

R2: Is de schaal zeven bij nummer drie lager dan de schaal bij nummer vier?

O: Nee. Je moet dat gewoon in relatie tot de rapportcijfers zien.

R2: In dit geval dan een neutraal voor ability en een zes.

O: Waarom wordt het dan een zes?

R2: Ja goede vraag. Misschien heeft het toch wel te maken met de bekwaamheid van de leverancier, ik zou er toch maar een vier van maken.

O: Een vier en dan wel een zes houden?

R2: Nou en een zeven toch maar, het kan best wel wat impact hebben. Dus doe maar zo. En het zelfde geldt voor welwillendheid.

O: Ook een vier?

R2: Ja. En integriteit ook, maar die mag dan wel hoger zijn, een acht of een negen.

O: Dus allemaal vier, vier, vier, of wil je... vier vier vijf, zeven, zeven, acht?

R2: Ja doe dat maar.

O: En waarom is integriteit iets hoger dan?

R2: Ja gevoelsmatig is dit ook een integriteitstekwestie dus euh ja als ze het niet zo nauw nemen met de regels, zullen ze het hier ook wel niet zo nauw nemen, dus ik denk dat je hier meer risico loopt. Dit is wel heel erg een gevoels iets en dit kan ik niet heel erg baseren op ervaring, dit stukje.

O: Oke, even kijken, bekwaamheid op opportunistic behaviour. Deze drie punten mag je als een zien.

R2: Oke, nou hier zie ik wel een sterke relatie met integriteit, dus ja dat zou ik een vijf geven en een negen.

O: En waarom?

R2: Nou ja hieruit blijkt, dat als ze zo gaan doen dat ze helemaal niet welwillend zijn en dat ze gewoon niet integer zijn.

O: Je zegt nu welwillend, dus welwillend is ook een sterke..

R2: Nee, nee, nee, op voorhand heb je bedacht dat zo'n partij bekwaam is, welwillend en integer, maar als ze nu allerlei dingen doen die niet kloppen dan zijn ze gewoon niet integer.

O: Ja, maar je noemt welwillendheid en integer net in een zin, dus dan geldt dit ook voor welwillendheid?

R2: Nee

O: Zo bedoelde je het niet?

R2: Nee.

O: Zie je een relatie tussen welwillendheid en opportunistic behaviour dan?

R2: Nee eigenlijk minder.

O: Waarom niet?

R2: Volgens mij gaat dit puur om de boel te belazeren. Dat is volgens mij puur een integriteit kwestie, maar aan de andere kant. Ze zijn dus veel minder welwillend dan gedacht, dus zo gezien loop je daar een risico. Met welwillend denk ik vooral aan de mate waarin mensen enthousiast zijn, maar de boel belazeren is echt een ander iets.

O: Welwillendheid is niet alleen de mate waarin mensen enthousiast zijn, maar welwillendheid is ook de mate waarin de leverancier het voor de klant goed wil doen.

R2: Ja dan zit daar ook gewoon een vette dingetjes. Dus dan ook hetzelfde.

O: Dus ook een vijf en een?

R2: Negen.

O: Oke en bekwaamheid?

R2: Nah als je zo doet dan ben je niet bekwaam. Dus daar zit dan ook een relatie in. Dus een vier en een zeven.

O: Gaan we door naar de volgende, security and privacy breach.

R2: Ja heeft volgens mij ook wel met ability te maken. Ik zou zeggen een vier en een zeven.

O: Waarom? Een korte toelichting?

R2: Ja om de zaken goed te beveiligen moet je wel weten waar je mee bezig bent dus dat is zeker een vaardigheid. En dus als blijkt dat ze op dat punt minder scoren dan verwacht dan loop je daar een risico.

O: Een redelijk groot risico zeg je dan he? Een zeven.

R2: Ja. En hetzelfde geldt voor welwillendheid. Euhm.. ja ook. Dat is een van de onderdelen die wel komen te vervallen als ze het niet zo goed met je voorhebben.

O: Dus een vier ook en de invloed?

R2: Ook een zeven.

O: en integriteit?

R2: ook hetzelfde.

O: En een korte toelichting op de integriteit?

R2: Eigenlijk hetzelfde, ik zie hier niet veel verschil tussen de onderdelen van vertrouwen. Ik denk dat de security gewoon een combinatie is van welwillendheid, vaardigheid en integriteit. Alle factoren zitten erin.

O: Daarom benoem je ze ook hetzelfde? Oké, even kijken dan gaan we door naar het volgende stukje, single / double moral hazard.

R2: Het speelt zeker een rol.

O: Bekwaamheid?

R2: Euhm.. nou die iets minder, denk ik. Ja die denk ik neutraal.

O: En waarom denk je iets minder?

R2: Ik denk dat niet zo zeer bekwaamheid met moraal te maken heeft.

O: En de invloed die het dan zou hebben?

R2: Ja dat is een zes. Ik denk dat welwillendheid wel een rol speelt, dus eens en dan een zeven.

O: Waarom?

R2: Nou ja, ik denk dat je als je bij welwillendheid schijnt ook elkaars belangen te behartigen een rol en dat heeft hier ook mee te maken en integriteit ook.

O: Ook een vier?

R2: ja, maar misschien nog wel iets meer dan, een acht ofzo.

O: Waarom die iets meer dan?

R2: Ik denk dat het een onderdeel van integriteit is dat als je ook gewoon voor een ander denkt zeg maar, dat is misschien wel een beetje een vaag antwoord. Kun je er wat mee?

O: Jawel, daar kan ik wel wat mee.

R2: Nee ik merk het inderdaad bij op het moment dat je zaken uitbesteed bij een andere partij, dan maken we ons op een gegeven moment geen zorgen meer. En dan bestellen we er een veelvoud van inderdaad of we gaan inderdaad minder zorgvuldig om met, want het wordt toch geregeld.

O: Ja.

R2: Dus ja dat is wel een puntje van aandacht vind ik, maar dat zit dan vooral op de welwillendheid en de integriteitsvlakken en niet zozeer op bekwaamheid.

O: Goal incongruence?

R2: Ja ik denk dat dit vooral te maken heeft met welwillend, euh ook wel met integriteit, maar het minst met ability. Dus ik zou zeggen met ability oneens.

O: Twee dan?

R2: Ja en dan een vier ofzo. En welwillendheid zo ik zeggen geheel eens.

O: En waarom?

R2: Ja het is ook een kwestie van gunnen, als je mensen naar een ander bedrijf gaan en je maakt daar afspraken over, je wilt natuurlijk als die mensen een doel hebben dat je dat dan ook meeneemt. Maar dat hangt ook af van de gunningsfactor. De welwillendheid van het bedrijf.

O: Het is niet alleen de mensen die over gaan, maar ook de zittende mensen. Daar moeten ze ook voor zorgen dat ze de persoonlijke doelstellingen halen.

R2: Ja. Dus dat is de belangrijkste factor, dus geheel en een acht ofzo. En integriteit in deze is natuurlijk ook belangrijk. Ik zou ook zeggen geheel eens, als dat niet klopt dan gaat het ook mis uiteindelijk, dan is de impact misschien iets minder. Een acht dan.

O: Dat is dan hetzelfde.

R2: Oh is dat hetzelfde dan..

O: Welke wil je dan hoger of lager?

R2: Euh, doe dan maar een zeven.

O: Even kijken, de laatste. De supplier employees have poor communication skills?

R2: Ja weet je het woord vaardigheden geeft wat mij betreft aan dat het om ability gaat. En als ze de vaardigheden niet hebben, maar wel de welwillendheid, daarom lukt het niet. Dus vanwege het woordje skills zou ik zeggen dat het vooral met ability van doen, maar het kan natuurlijk zijn dat als ik de organisatie vertrouw op welwillendheid dat ik onbewust denk dat ze ook vaardig zijn. Dus als ik ze inschat op welwillendheid en ik denk dat ze daarmee kunnen communiceren, dat is dan eigenlijk mijn eigen inschattingsfout. En dat zou ook zomaar kunnen ontstaan.

O: Of dat ze zich heel welwillend voordoen en je denkt dat komt wel goed.

R2: Ze zijn misschien ook wel heel welwillend. Maar dat verdoezeld gebrek aan kwaliteit op dit vlak, als je er al naar had gekeken moet ik zeggen, want je neemt ook niet alles mee. Dus in die zin denk ik dat je een risico loopt op in ieder geval ability en ook op welwillendheid.

O: Dus allebei geheel eens dan? Met de stelling? Of een vier?

R2: Ja doe maar een vier.

O: En integriteit?

R2: Ja ook, want het kan ook zijn, dat ze het ook min of meer hebben verdoezeld, ook eens en allemaal een acht denk ik.

O: Waarom allemaal een acht? Waarom zo'n hoge invloed?

R2: Nah ik vind het wel een belangrijke vaardigheid, dus de impact is voor mij ook wel groot.

Einde interview

11.8.3 Respondent 3

1. Formele vragen bij start van het interview

Opmerking: dit is een gestandaardiseerde tekst en geen letterlijke transcriptie. De onderzoeker leest onderstaande vragen voor:

- Dit gesprek wordt opgenomen, geeft u hier toestemming voor?
- Deelname van dit onderzoek is vrijwillig en indien u wilt stoppen kunt u dit te allen tijde aangeven. Stemt u toe om mee te werken aan dit onderzoek?
- De resultaten van dit interview worden anoniem verwerkt in een openbaar eindverslag. Geeft u toestemming om het resultaat van dit interview te verwerken in een openbaar eindverslag?

2. Introductie onderzoek

Hier wordt door de onderzoeker het onderzoek uitgelegd. Niet getranscribeerd.

3. Begrippen doornemen

De begrippen zoals deze zijn toegestuurd voor aanvang van het onderzoek worden met de respondent besproken. Aan de hand hiervan stelt de onderzoeker vast dat de begrippen overeenkomen met de visie van de respondent over deze begrippen. Niet getranscribeerd.

4. gegevensverzameling

De wijze van vragen stellen en te geven antwoorden worden met de respondent besproken en de onderzoeker geeft een voorbeeld van een vraag/antwoord. Niet getranscribeerd.

Vanaf het moment dat de vragen met betrekking tot de relatie tussen de factoren van trustworthiness en de ITO-risico's worden gesteld is het letterlijk getranscribeerd.

O: Is onderzoeker

R3: Is respondent 3

O: Is de factor bekwaamheid van toepassing op het risico backlash from internal IT staf?

R3: Minder ten opzichte van de andere twee.

O: Even kijken, dan zeg je minder, maar ben je dan geheel oneens of oneens?

R3: Als je kijkt naar de backlash from internal IT staf die dus niet over gaat naar de leverancier, die in de toekomst mogelijk hun baan.. dat vind ik vooral iets emotioneels. En ik denk dat die eerder aanslaan op zaken als integrity en welwillendheid. Ik denk dat dat meer de relatie beïnvloed dan de ability. Want daar zit een stukje onzekerheid bij en die ga je niet weghalen door de ability van de IT-leverancier.

Eigenlijk geheel oneens. Als je echt duidelijke uitslagen wil dan zou ik op de likertschaal 1 doen.

O: Dan heb ik ook geen rapportcijfer he, want dat is dan niet van toepassing, want als je geheel oneens bent met de stelling dan is er ook geen invloed op het geheel aan vertrouwen.

R3: Ja dat klopt.

O: Helemaal goed. Dan krijgen we dus de welwillendheid.

R3: Ja, ik denk dat die wel van invloed heeft en ik denk dat die vier is en het rapportcijfer is zeven. En de integrity die heeft daar... die zou ik dan een vijf geven op de schaal van Likert en een negen als rapportcijfer. Moet ik het ook beargumenteren?

O: Graag.

R3: Kijk, we hebben hier een situatie dat mogelijk de interne medewerkers over moeten naar de IT-leverancier, dat is een onzekere situatie, met een bepaalde mate van welwillendheid kun je een stukje van die onzekerheid wegnemen. Dus de backlash reduceert, maar ik denk dat al mensen zien dat er echt integer gedrag vertoont wordt en het is nog geconcretiseerd, wat dan verstaan wordt onder integrity, consistentie, eerlijkheid en openheid. En met name die openheid, dus transparantie, daar haal je die onzekerheden mee weg en daar dwing je ook respect mee af en daarom denk ik dat dat de grootste factor is om de backlash mee te reduceren.

O: Helder.

R3: Beetje op deze voet doorgaan?

O: Ja helemaal goed. Dan door naar de volgende. Is bekwaamheid van toepassing op contractual risk.

R3: Ik denk voor ability dat die er zeker wel is, want alles met contracten heeft voor een gedeelte te maken met inhoudelijke kennis rondom aanbestedingen en dergelijke en inhoudelijk ook de contracten die je met elkaar hebt afgesproken en de rechtsgeldigheid, de rolverdeling en hoe breed je dat hebt beschreven. Dus ability heeft daar absoluut betrekking op, dus ik zou die zeker wel, als je kijkt naar.. betrekking tot de contracten.. dan zijn er denk ik twee echt belangrijk en dat is de ability en de welwillendheid en die zou ik dan allebei op.. ability op vier zetten en de welwillendheid op 5. En die ability zou ik dan een rapportcijfer geven van acht en waarom omdat, nogmaals, je moet echt

verstand van zaken hebben om goed, gedegen en duidelijk een contract met elkaar af te stemmen om gedoe in de toekomst te voorkomen. En hoe concreet moet het zijn, zijn er relevante zaken etc.. En als het gaat om welwillendheid, ja bij de uitvoering van een contract helpt het heel erg voor de relatie als je voelt dat de ander wel van goede wil is. En ik denk dat je daarmee het risico op contractbreuk en contractgedoe echt aanzienlijk kan beperken. Dus als je ziet dat de ander zijn best doet en om daar, goed naar je luistert en daarmee aan de slag te gaan.. dus die zou ik dan een rapportcijfer negen geven.

O: En integriteit?

R3: ja integriteit, ook. Eerlijkheid en openheid natuurlijk. Die zou ik ook een vier doen, wat ik denk dat welwillendheid... je kan niet welwillend zijn en niet integer. Dat lijkt mij gewoon... een gekke combinatie, snap je?

Dus ik denk dat als mensen welwillend zijn dat ze dat vanuit een integer perspectief doen. Dus daarom denk ik dat in dit specifieke geval welwillendheid zwaarder weegt dan integriteit, omdat het in de slipstream zit. Dus ik zou die een vier en een acht doen, wel belangrijk, maar bijna inherent aan.

O: Je hebt de welwillendheid ook een acht gescoord he, maar dan heb je een vijf en een acht.

R3: Ja, je zou daar op basis van mijn verhaal, meer onderscheid in zien? Ik snap wat je bedoeld, omdat het zo dicht tegen elkaar aan ligt, welwillendheid en integriteit. Waarbij welwillendheid de belangrijkste factor is, kun je zeggen dan moet je ze misschien anders beoordelen, maar omdat het zo dicht tegen elkaar aan ligt is er ok wat voor te zeggen om ze dicht tegen elkaar een te waarderen.

O: Oké is prima.

R3: Volgende?

O: Ja

R3: Coördinatie tussen cliënt en leverancier. Daarbij is ability zeker belangrijk, want het gaat om vaardigheden, sociale vaardigheden onder andere en administratieve vaardigheden, die zijn daar wel van belang. Want als jij gewoon, we weten het allebei, netjes op tijd geïnformeerd wordt en dat je dus een bekwaam counterpart hebt, dan helpt dat al in de coördinatie. Dus volledig mee eens, vijf, en als dat goed werkt denk ik dat dat een tien is in de coördinatie, omdat dat namelijk er voor zorgt dat de informatie ongevraagd en zonder rappelleren naar je toe komt.

O: En dat werkt dus ook de andere kant op, stel dat iemand die vaardigheden niet heeft dan heeft dat dus enorm veel invloed op je vertrouwen. De mate van vertrouwen gaat dan naar beneden.

R3: Ja, want dan kan je dus niet meer vertrouwen dat je het juiste antwoord op de juiste tijd krijgt en dus ja, ga jij op basis van dat mindere vertrouwen dus zelf lijstjes bijhouden en continue rappelleren.

O: Ja

R3: Dus ik denk van die drie ja, want welwillendheid, ja onder tijdsdruk of iemand is niet vaardig genoeg, nogmaals, die begrippen liggen natuurlijk wel erg in elkaars verlengde. Een welwillend iemand die niet capabel is die gun je misschien wel op persoonsniveau, wel oké ik kan niet boos op hem worden, maar je wordt er wel een beetje gek van. Die zou ik dan op oneens doen.

O: Oneens? Dus dat hij niet van toepassing is op het risico?

R3: Op de lange termijn wel.

O: Dus een 2, dus er is dan nog wel enige.

R3: Moet ik hem dan waarderen?

O: Ja

R3: Een vijf. Waarom ik hem dan niet op 1 of 2 waardeer, omdat in de aanloop, dat je op basis van iemands welwillendheid niet gelijk het vertrouwen beschaamt, als je ziet dat iemand welwillend is, maar structureel wordt dat niks natuurlijk.

Dan integriteit, die is erg belangrijk. Als jij onjuiste informatie krijgt of men komt zijn afspraken niet na, zonder dat, dat te maken heeft met welwillendheid of bekwaamheid. Dus die zou ik ook op vijf zetten en een 10, want dat gaat gelijk gedoe opleveren.

Culturele verschillen, die herken ik zeker, die hebben invloed op de vertrouwensrelatie. Die probeer ik even te relateren aan de drie aspecten van trustworthiness. Dan ga ik er even vanuit dat beide

partijen bekwaam, welwillend en integer zijn, dan kun je nog steeds cultuurverschillen hebben. Dat je gewoon andere ideeën hebben over....

O: Het gaat om de perceptie wat je hebt van je leverancier he. Dus de perceptie met betrekking tot bekwaamheid, integriteit en welwillendheid. Die drie factoren maken dat jij je leverancier vertrouwt of niet vertrouwt.

R3: Gaat het dan erom in welke mate culturele verschillen in dit geval invloed hebben op..

O: Nee

R3: Andersom he?

O: In welke mate bekwaamheid invloed heeft op het risico culturele verschillen.

R3: Op culturele verschillen?

O: Ja tussen klant en leverancier.

R3: Nou ability denk ik niet zo, wel welwillendheid en integriteit.

O: Dus niet zo of helemaal niet?

R3: Het heeft namelijk te maken met normen en waarden, culturele verschillen. En ik zie dan bekwaamheid zie ik daar minder dicht aan liggen als welwillendheid en zaken als openheid, eerlijk en consistentie.

O: Ja dus bekwaamheid, geheel oneens?

R3: Ja geheel oneens.

O: En welwillendheid dan?

R3: Dat vind ik wel echt een cultureel aspect, dat heeft te maken met klantgerichtheid of je open stellen voor.

O: Dus geheel eens dan?

R3: Ja en ik denk dat als iemand welwillend is dat die ook wil luisteren, dus van goede wil is, dan zou ik dat wel een negen zeggen. En integriteit is natuurlijk ook een belangrijk aspect, dat ligt zo dicht tegen de normen en waarden aan, die dus ook een vijf en die zou ik misschien wel een tien euh..

O: Waarom dan een tien?

R3: Euh... nou ja als je cultuur definieert als de breed gedragen normen en waarden, en rituelen symbolen en alles wat erbij komt kijken, dan is welwillendheid gaat over intentioneel gedrag, maar integriteit dat zit dieper in het DNA van de organisatie en dus ook in jou als persoon. Dat stuurt veel meer de mate waarin je je gedrag ten toon spreidt. Bijvoorbeeld op zaken als consistentie, eerlijkheid en openheid in dit geval. Dus ik denk dat dit misschien nog wel meer van invloed is dan welwillendheid. Vandaar dat onderscheid.

O: Ja.

R3: Difficulty in managing remote teams...Dan zijn al die drie factoren belangrijk als je het hebt over offshoring. Omdat namelijk, als een van die drie factoren onvoldoende is dan heb je veel minder mogelijkheden om dat onsite.. dus dit moet veel beter op orde zijn om die relatie goed te laten werken met een offshore team.

O: Dus welke score zitten we dan?

R3: Dan zou ik ability en welwillendheid hoger scoren, als hoogste, en ik denk dat ability misschien nog wel het hoogste is, want je hebt vaak te maken met contractuele afspraken en met een soort werkpakket wat je offshore weg zet, een soort ontwikkelwerk en dat krijg je terug. Dan hangt het er heel erg van af hoe bekwaam iemand is om jou specs te vertalen bijvoorbeeld. Nah en als dat goed gaat denk je he dat beïnvloed mijn vertrouwen, dat zijn wel bekwame mensen. Je weet helemaal niet of ze welwillend zijn, misschien worden ze wel geslagen door hun baas, maar ze zitten in India, dus dat zie je niet. Ik denk hier die bekwaamheid is echt geheel eens en die beïnvloed denk ik van de drie het meeste dus als je het goed het onderscheid wil aanleggen dan zou ik hier het cijfer tien voor geven en voor die welwillendheid die zou ik dan vier doen, eens. Ik denk dat die zeker een invloed heeft, maar dan een zeven of een acht. Doe maar een acht. En integriteit natuurlijk ook wel he, want ik zei dat ze alle drie belangrijk waren, dus die is ook eens. Die zou ik dan een zeven doen.

O: Ja

R3: En met name de consistentie is dan belangrijk.

O: van integriteit bedoel je?

R3: Ja, omdat je zo product gestuurd werkt. Ja wat zit daar voor een eerlijkheid aan, als je krijgt wat je hebt afgesproken, dat beïnvloed volgens mij meer de vertrouwensrelatie. Zou ik hebben dan he. Lack of trust?

O: Ja

R3: Hier is integriteit natuurlijk het meest belangrijk, want ja dat triggert gelijk een lack of trust, als iemand niet integer is, niet eerlijk, niet open en niet consistent. Dus dat is echt vijf en tien.

Dat is wel echt heel duidelijk te pin punten op dit aspect.

Welwillendheid misschien wel iets minder, maar vaardigheden denk ik wel, want vaardigheden bepaalt uiteindelijk toch in welke mate diegene levert wat je met hem hebt afgesproken. Iemand kan totaal niet welwillend zijn, omdat hij ruzie met zijn vrouw heeft of omdat hij niet zo lekker heeft geslapen, maar als hij toch elke keer zijn afspraken nakomt, dan heb ik toch vertrouwen in die persoon. Word ik niet blij van het feit dat ik voel dat hij niet zo welwillend is, maar ja dat beïnvloed dan minder dat aspect dan dat hij bekwaam is. Dat is ook meer in lijn met waar we het net over had, die coordination aspect. Dus dan zou ik ability of bekwaamheid hoger, dus dan zou ik daar een vier en een negen doen. En die welwillendheid, neutraal en een zeven. En waarom toch een zeven, ja als iemand dag in dag uit jaar in jaar uit niet welwillend is dan gaat het toch een beetje jeuken met je lack of trust. Want dan heb je namelijk elke keer zoiets van, wanneer gaat het omslaan.

O: Oké.

R3: Loss over control over data. Ja als dat echt moedwillig is, daar ga ik in dit geval dan vanuit, het moedwillig verstrekken van data aan andere, dan heeft dat vooral..

O: Het hoeft natuurlijk niet moedwillig te zijn.. Het kan natuurlijk ook aan incompetentie liggen natuurlijk.

R3: Ja als je het zo bekijkt nou dan heeft welwillendheid, als je met de beste wil van de wereld, het is veilig of niet, iemand is integer of niet, welwillendheid heeft daar weinig invloed op. Dus die zou ik geheel oneens doen, dus dan hoeft ik hem ook niet te scoren. Maar wat jij zegt, je moet dan wel.. als jou intentie is om geen verlies van data aan derden te veroorzaken dan moet jou ability hoog zijn, dus dan ben ik absoluut eens, zeker in een complexe infrastructuur, een vijf en een tien. En natuurlijk moet dat ook gelden voor je integriteit anders dan heb je natuurlijk.. Je moet wel eerlijk zijn.. en.. een vijf en een tien.

O: Bekwaamheid op opportunistisch behaviour?

R3: Dit heeft vooral te maken met welwillendheid en integriteit. Shirking heeft echt met welwillendheid te maken, het opzettelijk ondermaats presteren, je wil dus eigenlijk gewoon niet. Maar hij heeft ook een aspect met eerlijkheid, dus het is een combinatie van welwillendheid en integriteit, die zou ik dus allebei op .. Dan zou ik welwillendheid op vier doen en acht en integriteit op vijf en negen. En waarom er zit iets opzettelijks in, dus dat heeft wat mij betreft niet zo veel met.. ja je moet wel de vaardigheden hebben om niet integer te handelen of opportunistisch te handelen, maar dat is volgens mij niet de doelstelling van dit risico.

O: Waar komt bekwaamheid dan op? Geheel oneens bedoel je?

R3: Ja, wat mij betreft geheel oneens. Je moet wel bekwaam zijn om free-ride gedrag te vertonen, maar goed dat komt vooral voort uit beperkt integer gedrag en de welwillendheid om dat gedrag te vertonen.

O: Ja, even kijken. Bekwaamheid op security of privacy breach?

R3: Nou hier is nou net ability, vaardigheden, wel belangrijk, want het is echt een vak om complexe omgeving veilig te houden. Dus dat is echt vijf en tien, zeker bij deze.

O: Waarom geef je die een tien dan? Waarom die zo hoog is?

R3: Vanwege de inhoudelijke kennis die nodig is en die als iemand kan aantonen dat die zoveel verstand van zaken heeft dan beïnvloed dat mijn vertrouwen. Neem bijvoorbeeld een [naam van een medewerker], als ik bij hem het gevoel krijg, ik ken de materie door en door en ik heb allemaal soorten cursussen gevolgd en ik heb er ervaring mee en ik weet hoe we al die aspecten en aanvallen moeten tackelen, dan vind ik zijn welwillendheid en zijn integriteit helemaal niet.. minder relevant

voor onze vertrouwensrelatie. Als hij als autoriteit, want daar gaat het dan om. Autoriteit en dat zie ik dan vooral voor bekwaamheid en natuurlijk heeft dat ook iets te maken met integriteit, die zou ik ook vooral niet op een zetten. Welwillendheid, ja... doe die maar neutraal.

O: Met welke score dan?

R3: Doe maar een zes, want als iemand niet welwillend is dan heeft dat invloed op zijn motivatie en dan zakt toch zijn aandacht niveau en dan heeft dat toch effect op.. nou ja bent wel bekwaam, maar je gedrag.. laat dat niet zien.

O: Ja

R3: En iemand kan heel bekwaam zijn, maar als hij niet integer is dan heb je kans dat hij zijn bekwaamheid gaat inzetten voor andere dingen. Die gelijk het vertrouwen beschadigen. Dus die zou ik dan eens doen en een acht.

Single / double moral hazard, nou dit heeft ook weer met vooral de welwillendheid te maken denk ik. Er staat hier ook als een van de partijen zich niet optimaal inzet, wat mij betreft een op een welwillendheid. Dus die zou ik vijf en tien doen. Hoewel dat natuurlijk ook wel te maken heeft met een stukje eerlijkheid, dus die zou ik op vier en acht doen. Omdat het ook iets oneerlijks heeft, een beetje free-ride-achtige aspect.

O: Ja als je moedwillig het niet gaat inzetten..

R3: ja

O: En de bekwaamheid?

R3: Ja dat vind ik minder relevant. Dus die zou ik.. ik zie hem niet een, twee, drie, bekwaamheid. Ja dat heeft .. hij kan heel bekwaam zijn.. nee een één.

O: Ja. Bekwaamheid is die van toepassing op goal incongruence?

R3: Dat heeft met vaardigheden te maken, is iemand in staat om dat te zien, om het aan te voelen en om er adequaat mee om te gaan. Dus ik denk dat dat zeker een eens is en een acht. Hetzelfde geldt voor welwillendheid, die leverancier moet natuurlijk wel bereid zijn om dat te zien en daar de voordelen van eens. Ja ik moet dat reduceren en mee dealen. Dus dat zou ik dan ook vier en acht doen, volgens mij zij die dan wel gelijkwaardig. En het heeft volgens mij dan niet zo veel met integriteit te maken, omdat je het functioneel ziet, van ik weet dat er naast bedrijfsdoelstellingen ook persoonlijke doelstellingen zijn, daar moet ik in mijn relatie met mijn afnemer rekening mee houden, ja dat heeft wel iets met integriteit te maken. Je moet hem ook niet op lager dan drie zetten. Nou je zou die op vier en zeven kunnen doen.

O: Waarom een zeven?

R3: Euhmm.. misschien als je kijkt naar.. integriteit is gelimiteerd tot drie, consistentie, eerlijkheid en openheid van de leverancier. Je zou het aan eerlijkheid en openheid van de leverancier kunnen relateren. Eerlijkheid in die zin dat je het verschil van jouw neus, bij die specifieke persoon van die afnemer staat een beetje zus en een beetje zo, ja kan je het misschien onder eerlijkheid beschouwen om daar rekening mee te houden dat die persoon, nou ja om daar toch effectief mee om te gaan.

O: De laatste, bekwaamheid is die van toepassing op supplier employees have poor communication skills.

R3: Deze is lekker dicht bij huis in ieder geval. Dit heeft natuurlijk één op één met vaardigheden te maken, het gaat om skills. We kunnen hier niet anders dan vijf en tien zetten.

Het heeft natuurlijk ook wel met welwillendheid te maken. Dus die zou ik dan op vier en acht zetten, omdat ik hem iets.. omdat hij echt ingezoomd wordt op skills triggert mij dat om die ability hoger te normeren.

O: Je geeft een acht voor welwillendheid? Wat is de toelichting daarop?

R3: Om het echt te kunnen toepassen, communicatie vaardigheden, dan moet je het willen en kunnen. En ability en welwillendheid, die dekken het willen en het kunnen.

O: En integriteit?

R3: Dan hebben we het niet over de inhoud van de communicatie, dan vind ik dit wat minder. Dan zou ik die neutraal doen en zes.

O: Waarom?

R3: Nogmaals omdat het niet om de inhoud gaat van de communicatie, dus dat is dan geen aanleiding om die dan op hoog te zetten en je kan natuurlijk heel effectief communiceren, maar niet eerlijk. Misschien aan de consistentie, het is gek als er een medewerker de ene keer wel goed communiceert en de andere keer niet. Ik kan me voorstellen dat dat.. ja hoe komt dat, het is niet consistent. Is dat dan onderdeel van integriteit of ligt het aan de welwillendheid. Is deze medewerker de ene keer wel welwillend en de andere keer niet. Ja, in relatie tot die communication skills, dat vind ik dan lastig te interpreteren, gevoelsmatig zou ik hem zelfs helemaal op 1 zetten, als je echt naar skills kijkt. En weet je waarom? Oplichters die kunnen vaak perfect communiceren, waarom? Dat is voor hun heel erg belangrijk om hun doel te bereiken. Dat zegt niks over hun integriteit, het zegt wel iets over het feit dat ze heel gemotiveerd zijn om het te doen en dat ze ook de vaardigheid hebben.

O: Zullen we hem dan op één zetten?

R3: Ja, want anders wordt het een beetje een niks zeggend verhaal en dat is niet goed voor je onderzoek. Wat sterk is moet goed gescoord worden en wat vaag is dat euh..

Einde interview

11.9 Appendix 9: Overzicht van de afwijkingen van de beïnvloeding van de relatie.

In deze appendix is Tabel 10 opgenomen met in de tweede kolom de Likertwaarden die de respondenten hebben gegeven aan de stelling of de factor van trustworthiness van toepassing is op het ITO-risico. Daarnaast is er in de derde kolom, indien er een relatie gezien werd door de respondent, een rapportcijfer gegeven over de beïnvloeding van deze relatie op het totaal aan vertrouwen. De onderzoeker heeft opgemerkt dat deze beïnvloeding in veel gevallen een verdubbeling is van de Likertwaarde met een acceptabele afwijking van +1 of -1. In de vierde kolom heeft de onderzoeker de gegeven Likertwaarden verdubbeld. In de vijfde kolom staat de afwijking, het verschil tussen de vierde en vijfde kolom. De afwijkingen die meer dan één, zowel naar boven als beneden, zijn in dit overzicht geel gearceerd.

Tabel 10: Overzicht van de afwijkingen van de beïnvloeding van de relatie

Relatie uitgedrukt door de respondenten in Likertschaal waarde					Rapportcijfer gegeven door de respondenten van de invloed relatie				Likertschaal waarde verdubbeld door onderzoeker				Afwijking: Verschil invloed score / Likertschaal waarde verdubbeld			
	R1	R2	R3	R4	R1	R2	R3	R4	R1	R2	R3	R4	R1	R2	R3	R4
Is de factor ability van toepassing op Backlash from internal IT staff?	4	4	1	1	7	8	nvt	nvt	8	8	nvt	nvt	-1	0	nvt	nvt
Is de factor benevolence van toepassing op Backlash from internal IT staff?	4	4	4	4	9	7	7	8	8	8	8	8	1	-1	-1	0
Is de factor integrity van toepassing op Backlash from internal IT staff?	4	4	5	4	9	7	9	8	8	8	10	8	1	-1	-1	0
Is de factor ability van toepassing op Contractual risk	5	4	4	5	10	8	8	9	10	8	8	10	0	0	0	-1
Is de factor benevolence van toepassing op Contractual risk	5	4	5	4	10	6	8	7	10	8	10	8	0	-2	-2	-1
Is de factor integrity van toepassing op Contractual risk	5	4	4	5	10	7	8	9	10	8	8	10	0	-1	0	-1
Is de factor ability van toepassing op Coordination between client and supplier	4	2	5	5	6	3	10	9	8	4	10	10	-2	-1	0	-1
Is de factor benevolence van toepassing op Coordination between client and supplier	5	4	2	5	8	9	5	9	10	8	4	10	-2	1	1	-1

Appendices: Appendix 9: Overzicht van de afwijkingen van de beïnvloeding van de relatie.

Is de factor integrity van toepassing op Coordination between client and supplier	5	4	5	4		9	8	10	7	10	8	-1	0	0	-1
Is de factor ability van toepassing op Cultural differences between client and supplier	4	1	1	5		6	nvt	nvt	8		8	nvt	nvt	nvt	-2
Is de factor benevolence van toepassing op Cultural differences between client and supplier	4	5	5	5		8	9	9	9		8	10	10	10	-1
Is de factor integrity van toepassing op Cultural differences between client and supplier	4	4	5	4		9	7	10	6		8	8	10	8	1
Is de factor ability van toepassing op Difficulty in managing remote teams	5	4	5	5		8	7	10	9		10	8	10	10	-2
Is de factor benevolence van toepassing op Difficulty in managing remote teams	4	4	4	3		7	7	8	6		8	8	8	6	-1
Is de factor integrity van toepassing op Difficulty in managing remote teams	1	4	4	3		nvt	7	7	4		2	8	8	6	nvt
Is de factor ability van toepassing op Lack of trust	5	5	4	5		10	8	9	10		10	10	8	10	0
Is de factor benevolence van toepassing op Lack of trust	5	5	3	5		10	7	7	10		10	10	6	10	-3
Is de factor integrity van toepassing op Lack of trust	5	4	5	5		10	7	10	10		10	8	10	10	0
Is de factor ability van toepassing op Loss of control over data	5	4	5	5		8	7	10	10		10	8	10	10	-2
Is de factor benevolence van toepassing op Loss of control over data	5	4	1	4		8	7	nvt	7		10	8	nvt	nvt	-2
Is de factor integrity van toepassing op Loss of control over data	5	5	5	4		10	8	10	8		10	10	10	8	0
Is de factor ability van toepassing op Opportunistic behaviour	4	4	1	1		7	7	nvt	nvt		8	8	nvt	nvt	-1
Is de factor benevolence van toepassing op Opportunistic behaviour	5	5	4	4		9	9	8	8		10	10	8	8	-1
Is de factor integrity van toepassing op Opportunistic behaviour	5	5	5	5		9	9	9	10		10	10	10	10	-1
Is de factor ability van toepassing op Security / privacy breach	5	4	5	5		10	7	10	10		10	8	10	10	0

Appendices: Appendix 9: Overzicht van de afwijkingen van de beïnvloeding van de relatie.

Is de factor benevolence van toepassing op Security / privacy breach	5	4	3	3	8	7	6	5	10	8	6	6	-2	-1	0	-1
Is de factor integrity van toepassing op Security / privacy breach	5	4	4	4	10	7	8	8	10	8	8	8	0	-1	0	0
Is de factor ability van toepassing op Single / Double moral hazard	1	3	1	1	nvt	6	nvt	nvt	nvt	6	nvt	nvt	nvt	0	nvt	nvt
Is de factor benevolence van toepassing op Single / Double moral hazard	4	4	5	5	7	7	10	8	8	8	10	10	-1	-1	0	-2
Is de factor integrity van toepassing op Single / Double moral hazard	5	4	4	4	10	8	8	7	10	8	8	8	0	0	0	-1
Is de factor ability van toepassing op Goal Incongruence	1	2	4	4	nvt	4	8	6	nvt	4	8	8	nvt	0	0	-2
Is de factor benevolence van toepassing op Goal Incongruence	4	5	4	5	8	8	8	9	8	10	8	10	0	-2	0	-1
Is de factor integrity van toepassing op Goal Incongruence	2	5	4	4	4	7	7	8	4	10	8	8	0	-3	-1	0
Is de factor ability van toepassing op Supplier employees have poor communication skills	4	4	5	5	7	8	10	10	8	8	10	10	-1	0	0	0
Is de factor benevolence van toepassing op Supplier employees have poor communication skills	4	4	4	4	7	8	8	9	8	8	8	8	-1	0	0	1
Is de factor integrity van toepassing op Supplier employees have poor communication skills	1	4	1	1	2	8	nvt	nvt	nvt	8	nvt	nvt	nvt	0	nvt	nvt

1.1.10 Appendix 10: Percentages Likertwaarden per relatie

Tabel 11: Percentages Likertwaarden per relatie inclusief Likertwaarden per respondent

Relatie		Percentage antwoorden m.b.t. Relatie					Likertwaarden per respondent			
		geheel oneens (1)	oneens (2)	neutraal (3)	eens (4)	geheel eens (5)	R1	R2	R3	R4
Is de factor ability van toepassing op Backlash from internal IT staff?		50%	0%	0%	50%	0%	4	4	1	1
Is de factor benevolence van toepassing op Backlash from internal IT staff?		0%	0%	0%	100%	0%	4	4	4	4
Is de factor integrity van toepassing op Backlash from internal IT staff?		0%	0%	0%	75%	25%	4	4	5	4
Is de factor ability van toepassing op Contractual risk		0%	0%	0%	50%	50%	5	4	4	5
Is de factor benevolence van toepassing op Contractual risk		0%	0%	0%	50%	50%	5	4	5	4
Is de factor integrity van toepassing op Contractual risk		0%	0%	0%	50%	50%	5	4	4	5
Is de factor ability van toepassing op Coordination between client and supplier		0%	25%	0%	25%	50%	4	2	5	5
Is de factor benevolence van toepassing op Coordination between client and supplier		0%	25%	0%	25%	50%	5	4	2	5
Is de factor integrity van toepassing op Coordination between client and supplier		0%	0%	0%	50%	50%	5	4	5	4
Is de factor ability van toepassing op Cultural differences between client and supplier	50%	0%	0%	0%	25%	25%	4	1	1	5
Is de factor benevolence van toepassing op Cultural differences between client and supplier	0%	0%	0%	0%	25%	75%	4	5	5	5
Is de factor integrity van toepassing op Cultural differences between client and supplier	0%	0%	0%	0%	75%	25%	4	4	5	4
Is de factor ability van toepassing op Difficulty in managing remote teams	0%	0%	0%	0%	25%	75%	5	4	5	5

: Appendix 10: Percentages Likertwaarden per relatie

Is de factor benevolence van toepassing op Difficulty in managing remote teams	0%	0%	25%	75%	0%	4	4	4	3
Is de factor integrity van toepassing op Difficulty in managing remote teams	25%	0%	25%	50%	0%	1	4	4	3
Is de factor ability van toepassing op Lack of trust	0%	0%	0%	25%	75%	5	5	4	5
Is de factor benevolence van toepassing op Lack of trust	0%	0%	25%	0%	75%	5	5	3	5
Is de factor integrity van toepassing op Lack of trust	0%	0%	0%	25%	75%	5	4	5	5
Is de factor ability van toepassing op Loss of control over data	0%	0%	0%	25%	75%	5	4	5	5
Is de factor benevolence van toepassing op Loss of control over data	25%	0%	0%	50%	25%	5	4	1	4
Is de factor integrity van toepassing op Loss of control over data	0%	0%	0%	25%	75%	5	5	5	4
Is de factor ability van toepassing op Opportunistic behaviour	50%	0%	0%	50%	0%	4	4	1	1
Is de factor benevolence van toepassing op Opportunistic behaviour	0%	0%	0%	50%	50%	5	5	4	4
Is de factor integrity van toepassing op Opportunistic behaviour	0%	0%	0%	0%	100%	5	5	5	5
Is de factor ability van toepassing op Security / privacy breach	0%	0%	0%	25%	75%	5	4	5	5
Is de factor benevolence van toepassing op Security / privacy breach	0%	0%	50%	25%	25%	5	4	3	3
Is de factor integrity van toepassing op Security / privacy breach	0%	0%	0%	75%	25%	5	4	4	4
Is de factor ability van toepassing op Single / Double moral hazard	75%	0%	25%	0%	0%	1	3	1	1
Is de factor benevolence van toepassing op Single / Double moral hazard	0%	0%	0%	50%	50%	4	4	5	5
Is de factor integrity van toepassing op Single / Double moral hazard	0%	0%	0%	75%	25%	5	4	4	4
Is de factor ability van toepassing op Goal Incongruence	25%	25%	0%	50%	0%	1	2	4	4
Is de factor benevolence van toepassing op Goal Incongruence	0%	0%	0%	50%	50%	4	5	4	5
Is de factor integrity van toepassing op Goal Incongruence	0%	25%	0%	50%	25%	2	5	4	4
Is de factor ability van toepassing op Supplier employees have poor communication skills	0%	0%	0%	50%	50%	4	4	5	5
Is de factor benevolence van toepassing op Supplier employees have poor communication skills	0%	0%	0%	100%	0%	4	4	4	4
Is de factor integrity van toepassing op Supplier employees have poor communication skills	75%	0%	0%	25%	0%	1	4	1	1